Oklahoma Law Review

Volume 60 | Number 3

2007

Decrypting the Code of Ethics: The Relationship Between an Attorney's Ethical Duties and Network Security

Ash Mayfield

COMMENT

Decrypting the Code of Ethics: The Relationship between an Attorney's Ethical Duties and Network Security*

I. Introduction

Imagine that you represent a client in a major legal transaction with a substantial amount of confidential information. You have file cabinets to house and organize hard copies of files, and electronic files containing confidential client information. As a prudent professional, you have taken extensive steps to secure the physical infrastructure of your office—you have installed an intruder alarm security system, you have functional door locks and heavy-duty doors, you have security cameras, and you carefully screen employees. In fact, it would be reasonable to say that you have met the steps that would be taken by a reasonably prudent attorney in physically securing client information. By all outward appearances, your information is secure, and your ethical and common law duties have been satisfied.

Yet, a security problem still exists that could be the functional equivalent of an unlocked door, adorned with a plush red carpet and advertised by a neon flashing sign. Like so many others in your profession, you have a high-speed Internet connection, and a high-speed network that connects the computers in the office to each other, allowing office employees to quickly and efficiently perform such mundane tasks as sharing files and using network printers. And, unwittingly, like so many other attorneys, by establishing this seemingly benign connection to the outside world, you have forged a path toward your own financial destruction.

The first signs of disaster are clear but are unnoticed by you or any of your staff. Even though a simple procedure would have alerted you that a third-party "hacker" is probing your network, you are unaware of the monitoring and auditing procedures necessary to detect and prevent such activities, let alone what to do if an intrusion was detected. Thus, as you continue working, an undetected and unauthorized intruder uses advanced tools to scan your computers for weaknesses through your Internet connection. As the day lingers, the hacker has already gained enough information to access your networks, but will not do so—yet. He would much rather wait until you leave

---

* This writing is dedicated, with immeasurable love and admiration, to my wife, Lori, and my daughter, Haven Lee. Absent their unyielding support, patience, and passion, ever-present throughout my turbulent law school adventure, neither this work nor my graduation would have been possible.

for the evening, ensuring that his plans will not be interrupted. Patiently waiting, he watches eagerly as each employee begins to log off of the network and as network traffic slows to a crawl. The attack is at hand.

The first targets are the shared files and folders available on the network. Once a convenience and tool of efficiency for office employees, the files are now low-hanging fruit for the hacker. He finds interesting information within the files, including clients' personal records, case memos, and various tidbits of information that indicate the firm's strategies for the litigation at hand. Not wanting to miss anything, he copies all of these files to his computer.

Unfortunately for you, this is not enough to satisfy the hacker's appetite. The hacker knows that while the shared files and folders have important information, other important targets exist as well. Using credentials that give him administrative rights on the network, he gains access to additional, unshared files, gathering a tremendous amount of information. This includes files that contain the usernames and passwords for every user on the network.

Possessing information that his employer has asked him to provide, the hacker now takes steps to ensure that his identity cannot be discovered. He clears the security logs so that a detailed understanding of the order and method by which he completed his attack will be difficult, if not impossible, to ascertain. On an impulse, the hacker also installs an array of software applications that, unknown to you, will log keystrokes, record from the microphones, and capture images from the webcams installed on office computers. He also configures a remote connection so that he can easily gain access to your network in the future.

The results are devastating and not altogether unpredictable. Personal client information, including social security numbers, is sold to third parties, who use the data to establish lines of credit and fraudulently obtain money and merchandise in the client's name. Worse, information is returned to the hacker's employer, perhaps connected to the opposing party, which severely weakens or destroys the attorney's case, and costs the client millions of dollars. The client is furious, feeling betrayed, sickened, and compromised. The identity of the hacker will never be discovered, and he will never be brought to justice for his shameful acts. Nevertheless, there is one party upon whom blame can be placed—you.

Relying upon the rules of legal ethics, your former client claims that you improperly failed to take reasonable steps to secure your computer network from attack, thereby facilitating these events. The client relies upon the Model Rules of Professional Conduct, claiming that you failed to competently perform your duties[1] and that you impermissibly revealed client information

1. MODEL RULES OF PROF'L CONDUCT R. 1.1 (2003).

to a third party.[2] To your horror, the client is victorious; you are responsible to your former client for millions of dollars in damages.

This article argues that attorneys have a duty to take certain reasonable measures to secure their computer network. The failure to take such measures may result in breaching ethical duties owed to clients.

Part II provides an overview of information technology, as applied to the law office, with an emphasis on networking and hacking techniques that can result in unintended disclosure of confidential information. Part III explores the ethical duties owed by attorneys to clients, weighing strong and weak state models to discover the best computer ethics standards. Part IV analyzes Oklahoma as a model state for computer ethics. Part V weighs the probability and gravity of a hacking attack against the burden imposed upon an attorney to provide network security, concluding that an attorney has a duty to reasonably secure his electronic files, and offering specific, practical recommendations that attorneys should use to help fulfill this duty. This paper concludes with Part VI.

II. Defining Technology & the Electronic Law Office

An attorney must possess a basic understanding of networking to understand the steps that he or she must take to secure confidential electronic files. As more technology is incorporated into daily business, an attorney must be aware of weaknesses caused by the technology that might lead to a breach of an ethical duty. While an attorney cannot be expected to operate as a networking professional, it is imperative that attorneys understand at least a cursory level of computer technology used in the law office and how that technology may be reasonably secured. Furthermore, to adequately appreciate the network vulnerabilities of the modern law office, it is helpful, if not essential, to create an organizational structure by which the computer technology may be classified. In other words, since the attorney is ethically bound to take reasonable steps to ensure the nondisclosure of client information, it would be futile to discuss the steps that should be taken by an attorney to secure the attorney's network without first discussing and defining the technology associated with and commonly used in law office networks.

A. Law Office Technology and Wired Networks

In the modern law firm, computer networks are becoming more prevalent.[3] A study published by the ABA Legal Technology Resource Center in 2003

2. MODEL RULES OF PROF'L CONDUCT R. 1.6(a).

3. *See* AM. BAR ASS'N, 2006 ABA LEGAL TECHNOLOGY RESOURCE CENTER SURVEY REPORT: MOBILE LAWYERS 39-42 (2006).

showed local area networks and high speed Internet connections were nearly ubiquitous in medium to large firms.[4] In another study, 70% of firms used local area networks, 27% used wide area networks, 43% used the Internet, and 19% used an Extranet.[5] By 2006, 76.6% of attorneys across all firms used computer networks, an increase of 6.6%.[6] 95% of large firms use networks, the highest percentage of technological usage in the industry.[7] Further, 99% of attorneys use the Internet in their offices.[8] Since sharing files intra-office can increase productivity, it is no surprise that networking has become more common.[9]

Law office networks often contain routers, switches, remote access devices, and firewalls.[10] Routers are the "traffic cops" of the Internet that connect networks with other networks.[11] For example, when a user enters the name of a desired website into a browser, the computer's request is routed across the Internet, "hopping" from network to network, finally arriving at the appropriate location. Then, perhaps using an alternate path, information is routed back to the user. Because of this vital function, routers are the backbone of the Internet. Likewise, switches connect similar and dissimilar devices to form local intranets, which are sometimes referred to as local area networks.[12] Switches function like routers, directing traffic. However, switches are designed to be a lower-cost option to manage a single local network, as opposed to a network-to-network communication platform.[13] Routers and switches also facilitate the use of remote access equipment.

Remote access equipment allows an attorney to connect to files stored on his or her office network from somewhere else. For example, a law office might have several modems that allow users to establish dial-up networking connections to the office.[14] Likewise, remote access servers (RASs) allow

---

4. AM. BAR ASS'N, 2003 ABA LEGAL TECHNOLOGY RESOURCE CENTER SURVEY REPORT: LAW OFFICE TECHNOLOGY, at xi-xii (2003) (noting that in 2001, 96% of legal organizations with ten or more attorneys had a local area network, and most of the firms had a high-speed connection to the Internet).

5. BRENT D. ROPER, USING COMPUTERS IN THE LAW OFFICE 42 (4th ed. 2004).

6. *See* AM. BAR ASS'N, *supra* note 3, at 39-42.

7. *Id.*

8. AM. BAR ASS'N, 2004-2005 ABA LEGAL TECHNOLOGY RESOURCE CENTER SURVEY REPORT: MOBILE LAWYERS, at xi (2005).

9. *See id.*

10. *See* SUSAN YOUNG & DAVE AITEL, THE HACKER'S HANDBOOK—THE STRATEGY BEHIND BREAKING INTO AND DEFENDING NETWORKS 552-53 (2004).

11. *Id.* at 552.

12. *Id.*

13. *Id.* at 552-53.

14. *Id.* at 553-54.

attorneys to "tunnel" through another Internet connection and gain access to the firm's network through a virtual private network (VPN).[15] Alternatively, Microsoft Remote Desktop enables an attorney to remotely manage an office computer, using an efficient virtual environment.[16]

Attorneys are using remote access more frequently to access electronic office files.[17] According to a 2005 ABA survey, VPN use increased dramatically between 2002 and 2005, up from 19% to 25%.[18] Further, in 2006, VPN usage surged to 28%, with 49% of large firms using the technology.[19] The increased popularity of VPNs to access files remotely highlights the importance and convenience of remote access to the client files. Nevertheless, this convenience does not come without a cost.

While remote access can vastly increase productivity and convenience, it creates an inherent security risk. By allowing an attorney to connect to the office network from some computer outside the office, a computer in the office must be actively "listening" for the attorney to solicit a connection. The office networking equipment must also be configured to allow this type of outside connection. Because remote access solutions leave an "open door" in the office network to accept connections from the Internet, they inherently present security risks. As noted by the ABA, "if client documents can be retrieved remotely by the lawyer, then perhaps the materials also could be accessed by people not authorized to view them."[20] A firewall, which limits the type of connections that can be made from the Internet to a local network, can help minimize this risk.

Firewalls represent the primary means of protection against Internet hazards.[21] Like Roman Sentinels, a firewall scrupulously monitors communications that pass through the "door" from the network to the Internet. Technically, a firewall allows a law firm to "provide access control between networks and to mediate connection requests based on a preconfigured set of rules. . . ."[22] For example, a firm might configure a firewall to stand between the high-speed Internet connection and the rest of the network. The firewall will only allow specific types of information to be passed in and out. A more complex firewall can be configured to forward all or specific incoming traffic

15. *Id.*
16. *Id.*
17. *See* AM. BAR ASS'N, *supra* note 8, at xi.
18. *Id.*
19. AM. BAR ASS'N, *supra* note 3, at xiii.
20. *Lawyers Must Use Reasonable Care to Safeguard Electronic Client Files*, 22 Laws. Man. on Prof. Conduct (ABA/BNA) 236, 236 (2006).
21. *See* YOUNG & AITEL, *supra* note 10, at 104.
22. *Id.*

to a specific computer in the law office. Firewalls can be software or hardware based, and vary greatly in their cost and degree of security offered.[23] For example, some software firewalls are available with zero-cost licensing,[24] while other, more complex hardware firewalls require third-party vendor installations that can exceed $100,000.[25] Nevertheless, firewalls are essential to a secure network.

Nearly all law firms have some type of firewall.[26] Between 2004 and 2005, 70% of attorneys used either a hardware or software firewall.[27] Solo practitioners were behind the technological curve, with just over 55% using this protection.[28] However, in 2006, over 90% of firms used either a hardware or software firewall, with 89.2% of solo practitioners meeting this criteria.[29] These encouraging statistics may indicate increased awareness by the legal community of the need for network security.

Finally, an often overlooked but important subset of law office technology includes e-mail and metadata. E-mail has exploded upon the legal culture. In a 2005 ABA study, 84.3% of respondents indicated that they used e-mail for work-related activities at least once a day, while over 96% sent a work-related e-mail at least each month.[30] Of the attorneys that have used e-mail, 96.7% use the technology for "routine correspondence," which includes case status updates, client bills, court filings, and marketing material.[31] Further, a higher percentage of attorneys who use e-mail are sending attachments, up from 89% in 2005[32] to 96.6% in 2006.[33]

As the studies indicate, e-mail is an efficient means of electronic communication designed to transmit small, mostly text-based messages.[34] E-mail can be used to send text, pictures, and small files intra-office or to other users on the Internet. While not absolutely secure, e-mail can be configured

23. *See id.* at 107-08.

24. *See* Jim Calloway, *Who Is Reading Your Hard Drive Tonight?: Security with High Speed Internet Access and a Few Words About Passwords*, 71 OKLA. B.J. 1712, 1714 (2000).

25. Jason Krause, *Guarding the Cyberfort*, ARK. LAW., Spring 2004, at 24, 31.

26. *See* AM. BAR ASS'N, 2006 ABA LEGAL TECHNOLOGY RESOURCE CENTER SURVEY REPORT: LAW OFFICE TECHNOLOGY 34 (2006).

27. AM. BAR ASS'N, 2004-2005 ABA LEGAL TECHNOLOGY RESOURCE CENTER SURVEY REPORT: LAW OFFICE TECHNOLOGY 50 (2005).

28. *Id.*

29. AM. BAR ASS'N, *supra* note 26, at 34.

30. AM. BAR ASS'N, 2004-2005 ABA LEGAL TECHNOLOGY RESOURCE CENTER SURVEY REPORT: WEB AND COMMUNICATION TECHNOLOGY 51 (2005).

31. *Id.* at 52.

32. *Id.* at 53.

33. AM. BAR ASS'N, 2006 ABA LEGAL TECHNOLOGY RESOURCE CENTER SURVEY REPORT: WEB AND COMMUNICATION TECHNOLOGY 49 (2006).

34. *See id.*

with additional security measures, such as encryption, that makes an unintended third-party recipient less likely to be able to read the contents of the communication.

Metadata is hidden information that, unknown to the sending party, can sometimes be "mined" and used by the receiving party to learn things about the document or sender. Metadata can include somewhat innocuous information, such as the date and time that the file was created, the name and title of the author, and other information about the software license holder. However, metadata can sometimes be used to divulge revision history from some word processing documents, potentially revealing otherwise confidential information about the sending party. While metadata can easily be "cleaned" from a document using a free software tool released by Microsoft,[35] an attorney who sends a document containing metadata runs the risk of breaching client confidentiality.

B. Wireless Networks: Leaving the Front, Back, and Side Doors Open

While attorneys have used traditional wired networks for some time, wireless networks continue to be an emerging trend, especially in smaller law offices.[36] According to a 2005 ABA study, 23% of firms use wireless networks to either access the Internet or share files.[37] Surprisingly, while the study indicated only 2.2% of firms with over 100 attorneys used wireless networking to access the Internet, 11.1% of small firms took advantage of the technology.[38] While the overall percentage of firms using wireless technology decreased in 2006 to 17%, usage in small and medium sized firms surged.[39] According to this newer study, 41% of firms with between fifty and ninety-nine attorneys use wireless networks, while 37.9 percent of solo practitioners have employed wireless connections.[40] Wireless networks, however, are inherently less secure than traditional wired networks, and an attorney who seeks to use wireless networking should do so with caution.

Wireless networks present a new element to the network security equation: a lack of physical access is no longer a barrier to network entry. On a wired network, in order for attackers to gain access to an electronic file, they must either be directly connected to the physical structure of the internal network

35. The metadata removal tool can be found by searching Microsoft's website. *See* Microsoft Corporation, http://www.microsoft.com (search for "rhdtool.exe") (last visited Jan. 5, 2008).

36. AM. BAR ASS'N, *supra* note 8, at 46.

37. *See id.* at xiii.

38. *Id.* at 46.

39. AM. BAR ASS'N, *supra* note 3, at xi.

40. *Id.*

or gain access to the internal network by "tunneling" through the network's Internet connection. In other words, in a traditional law office network, the attacker must either have actual, physical access to the network wires and terminals inside the law office, or must gain access to the firm's files through the Internet connection. Conversely, in order for a person to connect to a wireless network, all that is generally required are the appropriate credentials, such as an encryption key, and a wireless signal.[41] This process is commonly referred to as "associating with" an access point. If hackers can associate with an attorney's access point, they can use that point as a staging ground for further attacks on the attorney's network, or try to access client files.

Wireless networking security concerns require an attorney who uses wireless networking equipment to take additional security precautions to avoid breaching ethical duties. For example, client information and attorney passwords could be compromised by a hacker with little technical expertise using a tool that performs "packet sniffing," in which hackers intercept and decode radio signals to facilitate access to the attorney's network.[42] Attorneys using "wireless clients,"[43] such as a laptop or PDA equipped with a wireless card,[44] must also be wary of "honeypots" and rouge access points which

41. Some administrators employ additional security, such as Media Access Control ("MAC") address filtering. MAC addresses are "a unique address assigned to a networking device upon its creation by the manufacturer." YOUNG & AITEL, *supra* note 10, at 581-82. However, a simple scan of the wireless network and the clients associated with it provide a hacker more than enough information to clone a MAC address and bypass this restriction. Tools to scan wireless networks are widely available and easy to use. *See generally id.*

42. In a lab test performed by this author, an access point was configured with a MAC address and an eight-character WEP password. (For an explanation of WEP, see *infra* note 358 and accompanying text.) By monitoring the wireless traffic with one network card and probing the access point with another network card, thereby simulating client communication on the network, enough data packets were captured to discover the wireless password in under ten minutes. Note that the speed at which this attack can be successful depends somewhat upon the amount of network traffic present. Networks configured to use newer WPA security are more difficult to circumvent than WEP networks, but vulnerabilities still exist. *See infra* note 359 and accompanying text. Nevertheless, newly developed variants of WPA have proven to be more secure and seem to be promising, especially when paired with RADIUS authentication. *See* YOUNG & AITEL, *supra* note 10, at 143-46.

43. The term "client" in this context differs from an "attorney's client." Generally speaking, when a device is associated with a network controller, such as a wireless access point, an authentication server, or a DHCP server, the device is considered a "client" of the network controller. *See id.*

44. Wireless security problems are not exclusively limited to laptop computers on wireless networks. Because the prevalence of personal administrative devices, such as PDAs, supporting wireless communication is increasing, the vulnerability of information contained on and transmitted through these devices must be examined. *See* DAVID MELNICK ET AL., PDA SECURITY 251 (2003); *see also* John Cox, *Uncertainty Reigns in a Wireless World*, NETWORK

attempt to lure the attorney into making a connection to a spoofed access point, thereby compromising the attorney's security.[45] Several other methods of attack also exist that allow an attacker to intercept confidential communications.[46]

Wireless network attacks are prevalent and expensive, and even networking professionals can fall victim to hackers. Whether from failure to incorporate adequate encryption, filtering, physical security, or otherwise, errors in the configuration of wireless networks have opened doors for attack. For example, "[i]n a 2005 FBI survey, 93% of respondents stated their enterprises had detected security breaches within the last twelve months. . . . [T]he average cost of each breach was approximately $78,000. . . . [Thus, security is] a practical necessity that has become a reality for today's wireless networks."[47] With such volume of wireless network attacks, determining what the appropriate level of security is for any given wireless network is an essential knowledge for attorneys who use wireless networks. It is then incumbent on attorneys to implement the necessary security protocols.

Complicating the problem is the reality that, while wireless networks have increased in popularity, many parties fail to secure their wireless networks altogether.[48] "Of 88,122 [wireless access points] scanned in 2003, 67% had not enabled security measures. A more recent survey estimates that some 80% of U.S. residential wireless networks will be classified as 'unsecured' by 2007."[49] Therefore, the attorney should ensure that the expected benefits of configuring and maintaining a wireless network are adequate to undertake the risk.

Thus, attorneys are faced with a myriad of considerations with respect to which networking hardware should be used, as well as which security should be employed. The security risks associated with a wireless connection must be weighed against the advantages of wireless connections, such as increased productivity and mobility. The chief ethical harm is the danger that confidential client files could be compromised. Because the gravity of this harm is substantial, and the benefits are minimal, attorneys should carefully

---

WORLD, Apr. 18, 2005, at 20 (describing how wireless security issues are becoming more prevalent due to sensitive information being stored on "unsecure[d] smart phones, PDAs, laptops and MP3 players").

45. *See* YOUNG & AITEL, *supra* note 10, at 174.

46. *Id.* at 585-89.

47. JOHN R. VACCA, GUIDE TO WIRELESS NETWORK SECURITY 164 (2006).

48. *See* Robert V. Hale II, *Wi-Fi Liability: Potential Legal Risks in Accessing and Operating Wireless Internet*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 543, 547 (2005).

49. *Id.* (footnote omitted).

consider whether wireless networks in the law office are a reasonable, prudent choice.

C. David v. Goliath: The Sophistication and Means by Which an Attorney's Computer Network May be Compromised

Attorneys are at an automatic numerical disadvantage in terms of network security. While there may be one person in the law firm responsible for ensuring network security, thousands of hackers on the Internet await an opportunity to gain access to the firm's computers. As a result, network security must be agile, versatile, and vigilant. In order to prevent all security compromises, the network administrator must block every vulnerability in every instance. In other words, the defender must be right one-hundred percent of the time, while the hacker need merely exploit one security flaw to cause substantial damage.[50] This is especially troubling for an attorney, whose strict ethical duties demand heightened performance.

Law firms, like all businesses, must understand what vulnerabilities exist in their networks. Specifically, a law firm must understand computer and network security vulnerabilities, as well as the steps and costs associated with implementing a more secure system.[51] Further, an attorney must understand the mindset and dangerousness of hackers to fully understand the duty to secure electronic files. Nevertheless, understanding hackers can be difficult.

1. Meeting the Enemy: Understanding & Classifying Hackers and Their Diverse Skill-Sets

At the outset, it is helpful to note that "hacker" is not a homogenous term. People engage in hacking for a wide array of reasons and with a diverse range

50. Security vulnerabilities allow a hacker to more easily compromise the security of a computer. Nevertheless, perhaps one of the more common (and easy to remedy) security flaws lies within the physical configuration of a network. Ideally, a network should be designed in a manner that separates the internal network from the Internet so that traffic from the Internet is filtered through a central, secure location before entering the internal network. For example, a router should be connected to the point of high-speed access to the Internet. The router should be internally configured so that the only systems that are not behind a firewall are those systems which need to be publicly accessed (such as web and e-mail servers). These publically accessible systems will need to be added to the DMZ (demilitarized zone), which is not protected by the firewall, or otherwise made available to specific types of network traffic. Using this configuration, if hackers breach the security of the web server, they must overcome additional challenges to access the systems behind the firewall. *See* T.J. KLEVINSKY ET AL., HACK I.T.: SECURITY THROUGH PENETRATION TESTING 39 (2002).

51. CATHERINE PAQUET & WARREN SAXE, THE BUSINESS CASE FOR NETWORK SECURITY 7 (2005).

of skill sets.[52] The hacker of least concern acts primarily out of curiosity, seeking only to determine what information is vulnerable, generally without taking overt steps to compromise the data.[53] The "clever" hacker attempts to gain access to protected information because gaining such access presents a challenge.[54] The most important difference between a "curious" hacker and a "clever" hacker is that the clever hacker, once the network security has been compromised, seeks to cause as much damage in as little time as possible to gain notoriety.[55] A third type of hacker, the "professional," is a discrete mercenary. This type of hacker is dangerous because he possesses the skill and desire to gain access to a network, acquire critical information, and leave few footprints.[56] Perhaps the most dangerous type of hacker to an attorney, the professional hacker possesses extraordinary skill, understands technology, and is often hired by a party to produce a specific result, such as acquiring confidential information or destroying electronic files.[57]

Another helpful model of classifying hackers is the "tier" method, which groups hackers by skill type. First-tier hackers include "programmers who have the ability to find unique vulnerabilities in existing software and to create working exploit code."[58] First-tier hackers are certainly the rarest, comprising what would be the tip of the hacking population pyramid. These hackers possess an extensive knowledge of networking and programming technologies, spend a good deal of time honing their skills, and have the capacity to work with other hackers to exploit security weaknesses.[59] Second-tier hackers "have a technical skill level equivalent to that of system administrators."[60] While their knowledge is less than first-tier, these hackers still have the capacity to inflict serious damage and understand networking technologies. They possess enough skill to launch a successful attack, but rely upon first-tier hackers to find the weaknesses.[61] The most common type of hacker falls within the third-tier classification.[62] These hackers, sometimes called "script kiddies," possess the least technical understanding, relying predominantly upon software compiled by more skilled users.[63] Despite their technical inferiority, third-tier

52. KLEVINSKY ET AL., *supra* note 50, at 15.
53. PAQUET & SAXE, *supra* note 51, at 9.
54. *Id.*
55. *Id.* at 10.
56. *Id.*
57. *Id.*
58. KLEVINSKY ET AL., *supra* note 50, at 10.
59. *See id.*
60. *Id.* at 11.
61. *Id.*
62. *Id.*
63. *Id.*

hackers can be highly annoying, dangerous, and "are not afraid to run untested scripts against networks without truly understanding what the scripts do and what the consequences may be. This . . . often leads to disaster, such as the unintended loss of information."[64] By understanding the types and motives of hackers, attorneys can begin to take affirmative steps to curtail their efforts. But, attorneys must also understand the methods that hackers use to steal confidential data.

2. The Anatomy of a Hacking Attack: How to Lose Your License in Several Easy Steps

Every attack must begin somewhere. At the outset, a hacker will probably know little about the architecture of the attorney's network or the type of security enabled therein. For this reason, one of the first things that a hacker will try to do is discover the architecture of the network. Often, this procedure is initiated with a "whois" query that identifies the "administrative contact, billing contact, and address of the target network."[65] A whois query also allows the hacker to gain information about the domain name server (DNS) structure of target, which can give the hacker hints about the number and type of computers on the network.[66] Since DNS servers contain important information that is used to route traffic on the Internet, the hacker will attempt to gain access to the "list" in the DNS server by using a "zone transfer."[67] If successful, the hacker will have a list of some computer names known to the DNS server.[68] This is helpful because the hacker can sometimes identify the function of a computer by its name. For example, if the computer is called "mailserver," the hacker will easily be able to identify its function as an e-mail post office. This allows the hacker to attack or ignore it accordingly.[69] Likewise, if the server is named "Client_Files," a hacker will not have to guess which machine contains confidential information.

After a list of machines is ascertained, the computers are "pinged," a process analogous to a person poking another to elicit a response, to see if the

64. *Id.* at 11-12.

65. *Id.* at 53. Although the "whois" command is natively available on unix-based machines, several utilities exist that provide this functionality for Microsoft Windows. *See id.*

66. Domain name servers ("DNS Servers") play a role in translating Internet names that are easy for people to use and remember, *e.g.*, www.google.com, to the IP (number) based system used by computers on the Internet. *See id.* at 54.

67. *Id.* at 55.

68. *See generally* KLEVINSKY ET AL., *supra* note 50.

69. Computer names should not indicate the function of the computer. When network names are consecutive or otherwise easy to guess, a hacker might be able to ascertain the identity of other network computers after the discovery of only one network computer.

target computer will answer.[70] If a computer responds, it is powered on and "listening" for communication. Thus, after a successful ping response, the hacker knows that the responding device is a viable target for an attack. Traceroute commands, which track each hop or turn that network traffic takes, can also be used to help decode the target network's architecture and determine which computers are present.[71]

Once the identity of network computers becomes known to the hacker, attempts can be made to identify the operating system installed on the target computer. By determining which operating system is installed, a hacker can get a better idea as to which vulnerabilities may exist, and how to directly target those vulnerabilities.[72] The leading tool used to perform this task is "Nmap," which "analyz[es] the response of the target's TCP stack to the packets [it] sends out."[73] In other words, the program measures the ways in which the servers respond to specific requests, guessing from this information which operating system is installed. This can yield spectacular rewards. If, for example, a Windows NT based server is present on the network, the hacker can immediately target a specific point, such as TCP port 139, which may allow the hacker to connect to the default file sharing system.[74] If the hacker can gain access to this service, he can access the shared files stored on that computer.[75]

After the operating system is discovered, the hacker uses the information to target specific ports or a range of ports. Once the hacker has a rough idea of the ports that are probably available, he will commence a "port scan" on the target computer, specifically targeting a range of suspect ports.[76] If he finds

---

70. KLEVINSKY ET AL., *supra* note 50, at 57. Ping attacks can, if excessive, use substantial resources and slow a network. *Id.* at 58.

71. For example, if there are different paths to different servers, this might hint at the existence of firewalls or other network topography.

72. *See* KLEVINKSY ET AL., *supra* note 50, at 60.

73. *Id.*

74. By attempting to guess passwords using brute force techniques, the hacker can gain administrative level security to entire folders, or even volumes of data. *See generally id.*; *see also infra* note 81 and accompanying text for information regarding brute force attacks.

75. This is a conservative result. In a more damaging scenario, the hacker might connect via the IPC$ share, steal the Windows password hash files, and use his computer to determine the administrator's password. After this password information is determined, the hacker can use the administrator's credentials to gain access to the computer much more easily. Also, since many computer users have a common username and password scheme for many online services, this security compromise could expose users to collateral attacks via Internet services. This may include, but is not limited to, snooping in Internet e-mail, purchasing items online, and managing bank account information. *See* KLEVINSKY ET AL., *supra* note 50.

76. Although a port scan can target all ports on a system (1 through 65,535), limiting the search reduces the time required to perform the scan. *See id.* at 60-63.

an open port, he may be able to use it to connect to a service hosted on the target computer,[77] leading him to other helpful information.[78] In addition, the hacker may research the open ports to discover if the port numbers are associated with specific programs. For example, if port 64,301 is open, it will be possible to deduce that the computer is running *pcAnywhere* software, which configures the computer to "listen" on that port.[79] This information is invaluable because the hacker can then search vulnerability databases for known security flaws and exploits present in the installed software.[80]

After potential security holes are identified, the hacker will either attempt to exploit a known security flaw in an application installed on the server, or will attempt a "brute force"[81] attack to attempt to connect to the server through an open port and service.[82] "Exploits" seek to take advantage of certain hidden weaknesses in the code of some software, while a brute force attack repeatedly tries a combination of characters to "guess" the credentials. A brute force attack is analogous to guessing the number on a combination lock one unit at a time. The advantage of using software to perform this type of attack is, in some cases, the computer can process tens of thousands of guesses per second. This may allow a hacker to crack a weak password. After the security has been defeated, the hacker may have access to confidential files and information, may delete or modify software installed on the computer, may access other computers on the network, or may install software designed to perform various recognizance or malicious activities.[83]

---

77. Ports are a logical means by which computers can communicate with one another. For example, the HTTP (hypertext transfer protocol), which is used while browsing the Internet, uses port 80 to send information back and forth. This standard is helpful because network administrators can allow traffic on port 80 to pass through the firewall and route to the web server without exposing the web server directly to the Internet. Ranging from 1 to 65,535, open ports can be exploited to allow access to unintended or unauthorized users. *Id.* at 60.

78. For example, when the hacker attempts to scan and connect to open port 21 for the FTP (file transfer protocol) service, the target computer will probably return "banner" data containing the service name and version number. *Id.* at 63.

79. *Id.*

80. Several websites have vulnerability databases, including, but not limited to, "Bugtraq lists, Packetstorm www.packetstormsecurity.org, and SecurityFocus www.securityfocus.com." *Id.* at 64.

81. A brute force attack uses the power of the computer to generate numerous attacks per time unit against the host computer, hoping to use raw processing power and probabilities to find the correct combination of usernames and passwords. *See generally id.* at 320-25.

82. *Id.*

83. For example, the hacker might install a keystroke monitoring application which can capture information typed by the user. *See id.* at 65-67. Other more subtle methods, such as social engineering, can also be used to acquire passwords. During social engineering, hackers prey on the weaknesses and gullibility of people to gain access to passwords and other

While there are many dangers associated with the use of technology, especially networks that are connected to the Internet, the reality of modern law practice dictates that attorneys will use computers in the law office. If attorneys were required to ensure absolutely that networks could not be compromised by a hacker, they would abandon the technology. Not only would the practice of law be hindered, but the reduction in efficiency would damage the relationship between the attorney and client. Because this perfect standard is not applied in modern law, the attorney must determine what steps must be taken to avoid running afoul of the duty of electronic file security.

III. Attorneys, Ethics, and Computers . . . Oh My! Analyzing the Model Rules of Professional Conduct

Discussions of ethics and professional responsibility conjure images of ambulance chasing, contingency fees, and sex with clients. While the old "common sense" interpretation and application of the rules of professional responsibility worked well for many years, the advancement of technology has muddied the ethical waters which are ill suited to topics such as e-mail, computers, and the Internet. In fact, even ethical drafters two decades ago could not have contemplated that computer technology would have developed and become so prevalent in the law office. Thus, states have been left with the monumental task of interpreting and applying old ethical regulations regarding confidentiality and competency to the modern realities of the electronic law office. Not surprisingly, results have varied. Because each state is free to adopt its own variation of ethical codes of conduct, no single bright line rule governs the conduct of attorneys with respect to computers and technology.

Nevertheless, a trend has emerged among state bar associations to issue advisory ethics opinions that help generally define an attorney's technological duties. While some states issue only general guidelines, other states have explicitly defined the rights and responsibilities of an attorney regarding specific subsets of technology, such as e-mail, unintentional disclosure, metadata, and electronic storage of client files. The dominant portions of the Model Rules of Professional Conduct that deal with these issues are Rules 1.1 and 1.6.

A. Attorney Competency & Model Rule 1.1

Under Model Rule 1.1, an attorney has a duty of competency, which includes possessing a basic understanding modern computer technology. Model Rule 1.1 provides that "[a] lawyer shall provide competent

---

confidential security information. *Id.*

representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[84] Traditionally, this rule required an attorney to possess an adequate level of skill and knowledge, facilitating adequate representation of the client. Nevertheless, with the increasing popularity of computer technology in the law office, the rule has been interpreted by a number of states as requiring knowledge of computer technology.[85]

An attorney's duty to understand technology varies, ranging from a duty to attend continuing education on technology to an affirmative duty to unilaterally learn and understand computer technology used in client representation. On the more lenient scale of computer competency, Florida law counsels continuing education may be necessary to help attorneys understand the risks associated with sending e-mail and other electronic communication.[86] New York has promulgated a more stringent standard than Florida, holding that "[r]easonable care may, in some circumstances, call for the lawyer to stay abreast of technological advances and the potential risks in transmission in order to make an appropriate decision with respect to the mode of transmission."[87] New York and Florida are substantially ahead of the ethical curve in directly rendering attorneys responsible for competent use of computer technology. Nevertheless, their narrow guidelines fail to encompass the wide range of technology that is used daily in the law office.

Arizona has issued a much stronger model for understanding Rule 1.1 compliance. The Arizona State Bar requires an attorney who uses electronic files to "be competent to evaluate the nature of the potential threat to client electronic files and to evaluate and deploy appropriate [computer security] to

---

84. MODEL RULES OF PROF'L CONDUCT R. 1.1 (2003).

85. *See, e.g.*, State Bar of Ariz., Comm. on the Rules of Prof'l Conduct, Formal Op. 05-04 (2005), *available at* http://www.myazbar.org/Ethics/pdf/05-04.pdf ("[A]n attorney or law firm is obligated to take reasonable and competent steps to assure that the client's electronic information is not lost or destroyed. In order to do that, an attorney must be competent to evaluate the nature of the potential threat to client electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end."); Fla. Bar, Prof'l Ethics Comm., Op. 06-2 (2006), *available at* http://www.floridabar.org/ (follow "Search" hyperlink; then follow "Ethics Opinions" hyperlink; then search for "06-2"); N.Y. State Bar Ass'n, Comm. on Prof'l Ethics, Op. 782 (2004), *available at* http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&TEMPLATE=/CM/ContentDisplay.cfm&CONTENTID=6871; *see also* N.Y. State Bar Ass'n, Comm. on Prof'l Ethics, Op. 709 (1998), *available at* http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&CONTENTID=6317&TEMPLATE=/CM/ContentDisplay.cfm.

86. Fla. Bar, Prof'l Ethics Comm., Op. 06-2.

87. N.Y. State Bar Ass'n, Comm. on Prof'l Ethics, Op. 782; *see also* N.Y. State Bar Ass'n, Comm. on Prof'l Ethics, Op. 709.

accomplish that end."[88] Thus, Arizona establishes a two-part test for computer competency: the attorney must be able to identify potential threats, and be able to correct any problems that are identified. Furthermore, the duty extends beyond requiring an attorney to act in accordance with what he or she knows firsthand, specifically requiring the attorney to consult an expert and to ensure ethical compliance.[89]

While some attorneys may criticize what seems to be a burdensome regulation, Arizona has made a bold and visionary decision to force attorneys competently into the next era of legal practice. Attorneys in Arizona can no longer argue that they are technically uneducated, and that they cannot, therefore, protect client files from hackers. Rather, the risk has been allocated to the party in the best position to employ network security and protect client files—the attorney.

In addition, some scholars recommend taking the duty of competency a step further, claiming it may not be enough for an attorney to merely *understand* the risks associated with the technology they currently possess if the technology is not adequate to meet the competency needs of the client.[90] Rather, attorneys should be aware of and deploy new technology as needed.[91] Attorneys must determine whether "their clients may be placed at risk simply because they are not making use of high technology that has become commonplace in their field. If there is risk in using a computer, there may also be a risk in not using one."[92] Thus, under this interpretation, attorneys would need to not only understand the technology and dangers associated with his or her own network, but also be continuously conscious of improvements in technology that could be an ethical necessity of modern, competent practice.

Some scholars have indicated that this duty extends even further, requiring an attorney to adopt technology promptly, adding a temporal element to the attorney's duty of competency. One noted commentator, Raymond Nimmer, suggests that attorneys who are slow to adopt generally recognized benefits available through the use of computers may run afoul of ethical requirements.[93] Thus, under these guidelines, an attorney must understand the dangers associated with the technology and the means by which the dangers can be remedied, determine whether additional equipment is or should be required to competently represent the client's interests, and act quickly to correct any

88. State Bar of Ariz., Comm. on the Rules of Prof'l Conduct, Formal Op. 05-04.

89. *Id.*

90. *See* JAMES V. VERGARI & VIRGINIA V. SHUE, FUNDAMENTALS OF COMPUTER-HIGH TECHNOLOGY LAW (1991).

91. *Id.*

92. *Id.*

93. RAYMOND T. NIMMER, THE LAW OF COMPUTER TECHNOLOGY 7-1 to -35 (1985).

problem. Therefore, the need for competency is ongoing, the duty is substantial, and technology in the law office is rapidly evolving.[94]

Court tolerance of technological ignorance is also evolving. In 1986, in the case of *People v. Barnes*,[95] an attorney relied upon past precedent to support his proposition at trial that the state statute of limitations prevented prosecution of his client for "bail jumping."[96] In the decision, the court acknowledged that a paper-based authentication of the authority cited by the attorney would have seemed normal, noting that "[i]f the three lower court cases discussing the statute of limitations as it relates to bail jumping were 'shepardized', no appellate court cases would be discovered. Similarly a search of [a local digest] for a higher court precedent would be fruitless."[97] Nevertheless, by using an electronic search technique, the attorney would have discovered a binding decision by a higher court that was dispositive on the issue.[98] Notably, the court found no fault on the part of the attorneys, reasoning that the omission was "understandable," because "the commonly used and most expedient research tools [were] not helpful in this instance" and electronic research techniques "may be unavailable to many attorneys who do not enjoy the luxury of computer-assisted research . . . ."[99] Today, the presence of the Internet in modern life is so prevalent that a modern court would probably not reach the same conclusion. Rather, if an attorney failed to substantiate the accuracy of a cited authority through electronic means, the attorney would likely run afoul of his evolving competency requirements under Rule 1.1.

On the other hand, in at least one case, the increased use of technology by an attorney facing discipline helped him receive a softer penalty after missing a client's filing deadline. In a 2001 hearing in Louisiana, an attorney faced disciplinary action when he missed a filing deadline and rendered his client's claim worthless.[100] Although he still incurred sanctions, the attorney's sanctions were reduced because he made a "timely good faith effort to make restitution or to rectify the consequences of misconduct," when he configured

---

94. *See* ROPER, *supra* note 5, at 32.

95. 499 N.Y.S.2d 343 (N.Y. Sup. Ct. 1986).

96. *Id.* at 346.

97. *Id.*

98. *Id.*

99. *Id.* ("For example, if one consults McKinney's annotations to CPL 30.10 under the topic 'bail jumping—continuing nature of offense,' the case is not listed. Nor is it cited in the annotations to Penal Law Sec. 215.56, 215.57, or 215.59. Finally, reference to 'limitations of prosecution—continuing offenses,' (Key # 149-150) in *Criminal Law, West's New York Digest*, 3d ed., does not reveal the *Martinez* decision.").

100. *In re* James F. Welch, La. Att'y Disciplinary Bd., 99-DB-087 (2001), *available at* http://www.ladb.org/NXT/gateway.dll/DB/2001-10-03_99-db-087.htm?fn=document-frameset.htm$f=templates$3.0.

a software "tickler" system to remind him of upcoming deadlines.[101] By taking this remedial action and embracing technology, the attorney positioned himself to operate his law office more efficiently while avoiding enhanced liability.

Computer technology in the law office is a modern reality, and it would be difficult to successfully argue that an attorney "competently" uses his computer equipment, in terms of the scope of representing the client, if the attorney fails to properly secure the office computers. While misunderstanding or remaining ignorant of security problems and electronic resources might have been acceptable two decades ago, modern courts might fail to sympathize with an attorney whose client's files were discovered because of the attorney's failure to competently secure a computer network. Additionally, an attorney's technological duties are not limited to competency; greater concern for many attorneys could arise from the duty of confidentiality.

B. Confidentiality & Model Rule 1.6

Rule 1.6(a) of the Model Rules of Professional Conduct provides that "[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent," including taking steps that could reasonably prevent the discovery of such information by a third person.[102] Model Rule 1.6(a) applies to all information obtained by the attorney from and about the client,[103] but the duty extends beyond a mere prohibition against *intentional* publication of confidential information. Instead, an attorney has an affirmative duty to take reasonable steps to prevent even inadvertent disclosure.[104] Specifically, Model Rule 1.6(a) imposes a duty to "act competently to safeguard information relating to the representation of a client against inadvertent or *unauthorized* disclosure [of confidential information]. . . ."[105] To satisfy this duty, the attorney "must take reasonable precautions to prevent the information from coming into the hands of unintended recipients."[106]

Generally, computer-related issues that arise in the context of Model Rule 1.6 relate to encrypted e-mail, unintended disclosure of confidential information, metadata hidden within files, and electronic storage of client files. While a healthy majority of states have issued opinions in the last decade regarding e-mail, and multiple others regarding metadata, the real wildcard in this equation is the procedures by which attorneys should electronically store

101. *Id.*
102. MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2003).
103. *See id.* R. 1.6 cmt. 3.
104. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999).
105. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 15 (emphasis added).
106. *Id.* R. 1.6 cmt. 16.

client files. If an attorney fails to take reasonable steps to secure his computer network, it could lead to unauthorized disclosure of confidential files. Thus, an attorney must enable and configure reasonable network security measures in order to prevent client information from unauthorized disclosure. Unfortunately, there is no bright line rule on this issue. Nevertheless, analysis of how other states have regulated the use of law office technology is still relevant, as it can be synthesized to form a proposed body of law regarding law office computer network security.

1. Weaker Security Model States

Some states have taken a permissive view of security and technology, imposing a weaker standard on attorneys who use computers in the law office. Nearly every state allows attorneys to communicate using unencrypted e-mail, and some states have reconsidered older rules to allow attorneys to adapt to changes in technology. As one example, overruling an earlier ethics opinion, the Committee on Professional Ethics of the Massachusetts Bar Association decided in 2000 that an attorney's use of unencrypted e-mail usually does not violate the duty of confidentiality per the Massachusetts Rules of Professional Conduct.[107] Holding that "[l]egal and technical hurdles to the interception of Internet e-mail give rise to a reasonable expectation [of privacy]," the committee reasoned that an attorney must take care to ensure that confidential information is not accidentally relayed to an incorrect recipient, that third parties do not have access to the client's e-mail, and that the client has not expressly requested encrypted communication.[108]

Likewise, in a 1998 ethics opinion, the Association of the Bar of the City of New York embraced the Internet as a valid and reasonable tool of legal professionals, finding that the Internet is not sufficiently "insecure as to prohibit an attorney from conducting any legal business whatsoever over it."[109] The New York City bar opinion held that communication via unencrypted e-mail is reasonable and permissible,[110] and the New York Legislature adopted that policy, changing a rule of civil procedure to state that privileged information does not lose its privileged nature merely because it was

107. Mass. Bar Ass'n, Comm. on Prof'l Ethics, Op. 00-01 (2000), *available at* http://www.massbar.org/for-attorneys/publications/ethics-opinions/2000-2007/2000/opinion-no-00-1.aspx.

108. *Id.*

109. Ass'n of the Bar of the City of N.Y., Comm. on Prof'l & Jud. Ethics, Formal Op. 1998-2 (1998), *available at* http://www.nycbar.org/Ethics/eth1998-2.htm.

110. *Id.* ("[A]lthough some early opinions expressed [the] view that unencrypted e-mail violated confidentiality rules, the prevalent view, which this Committee adopts, is that electronic transmission is in most instances an acceptable form of conveying client confidences even where the lawyer does not obtain specific client consent.").

transmitted electronically.[111] Noting that the criminalization of e-mail interception reduces the likelihood of interception,[112] New York state uses a sliding scale for security requirements depending upon the facts and circumstances surrounding the representation. Nevertheless, the attorney must still disclose to the client that e-mail is subject to interception by hackers.[113]

Connecticut's ethics panel took a pragmatic approach, analyzing whether e-mail could be used without violating the attorney's duty to take "every effort practicable to prevent disclosure" of confidential information.[114] Weighing the benefits of e-mail against the risks of disclosure, the panel determined that "[a] great deal of technical sophistication and a massive commitment of time and resources on a governmental scale" would be required to intercept an e-mail.[115] Further, the panel held, while it was feasible that e-mail could be intercepted, the risk was so low that attorneys may ethically communicate with a client via unencrypted e-mail.[116] After examining the risk of interception and burden of non-use, the opinion concluded that e-mail was a permissible tool, and did not violate the attorney's ethical duties.[117]

Misdirected e-mail or documents containing metadata can also lead to a breach of confidentiality. By scanning a document for hidden metadata, a receiving party can sometimes discover information that was inadvertently imbedded in a word processing document. As discussed in Part II, metadata can include innocuous data, such as the author of a document, or can include damaging information such as revision history that can reveal confidential information, including part or all of the trial strategy.

States in the weaker model differ somewhat regarding the duties of inadvertent recipients of electronic, otherwise confidential, information. Generally, the weaker model states place more of a duty upon the recipient of information disclosed unintentionally, thereby weakening what should be a duty upon the sending party to ensure that information is not accidentally disclosed. As one example, in a 1994 Maine ethics opinion, the Professional Ethics Commission of the Maine Board of Overseers of the Bar held that attorneys must give notice to an opposing party if they received what would

111. N.Y. C.P.L.R. 4548 (Consol. 2006).

112. N.Y. State Bar Ass'n, Comm. on Prof'l Ethics, Op. 709 (1998), *available at* http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&CONTENTID=6317&TEMPLATE=/CM/ContentDisplay.cfm.

113. Ass'n of the Bar of the City of N.Y., Comm. on Prof'l & Jud. Ethics, Formal Op. 1998-2.

114. Conn. Bar Ass'n, Comm. on Prof'l Ethics, Informal Op. 99-52 (1999), *reprinted in* PROFESSIONAL RESPONSIBILITY REFERENCE GUIDE: CONNECTICUT, at C-313 (2000).

115. *Id.*

116. *Id.*

117. *Id.*

otherwise be privileged information through inadvertent disclosure, if the attorney knew or should have known that the document should have been protected by an evidentiary privilege.[118] Nevertheless, this holding was reconsidered in 2000, in light of the facts in the case of *Corey v. Norman, Hanson & DeTroy*,[119] in which the Maine Supreme Court held that an attorney who receives obviously privileged data has an *affirmative* duty not just to notify the opposing counsel, but to return the wrongly disclosed evidence.[120] Likewise, the Professional Ethics Committee of the Florida Bar held that an attorney who is the recipient of an inadvertent, confidential disclosure has an affirmative ethical duty to notify the sending party and inform the party that the confidential information has been received,[121] while New Hampshire has adopted an ethics revision that requires attorney recipients of inadvertent disclosure, such as a misdirected e-mail, to "promptly notify the sender" in order to permit that person to take protective measures.[122]

A number of states have issued ethics opinions that deal with metadata directly. For example, the New York Bar Association considered the problem of metadata as early as 2001, holding that it is unethical for attorneys to use technology to harvest or attempt to harvest hidden data from documents or trace the origins of e-mail.[123] Likewise, Florida places a duty on the receiving party of documents and e-mail not to harvest or attempt to harvest metadata stored in the document on the receiving party.[124] Under both of these rules, the burden is upon the receiving party to refrain from discovering confidential material.

Weaker model states generally allow confidential client information to be stored electronically. The states in this group typically allow an attorney to use third-party vendors to service the computer systems upon which the confidential information is stored without violating the rules of confidentiality. Many of these states do not require attorneys to affirmatively secure

118. Me. Bd. of Overseers of the Bar, Prof'l Ethics Comm'n, Op. 146 (1994), *available at* http://www.mebaroverseers.org/Ethics%20Opinions/Opinion%20146.htm, *overruled by* Me. Bd. of Overseers of the Bar, Prof'l Ethics Comm'n, Op. 172 (2000), *available at* http://www.mebaroverseers.org/Ethics%20Opinions/Opinion%20172.htm.

119. 742 A.2d 933 (Me. 1999).

120. Me. Bd. of Overseers of the Bar, Prof'l Ethics Comm'n, Op. 172.

121. Fla. Bar, Prof'l Ethics Comm., Op. 06-2 (2006), *available at* http://www.floridabar.org/ (follow "Search" hyperlink; then follow "Ethics Opinions" hyperlink; then search for "06-2").

122. N.H. RULES OF PROF'L CONDUCT R. 4.4(b) (2007).

123. N.Y. State Bar Ass'n, Comm. on Prof'l Ethics, Op. 749 (2001), *available at* http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&CONTENTID=6533&TEMPLATE=/CM/ContentDisplay.cfm.

124. Fla. Bar, Prof'l Ethics Comm., Op. 06-1 (2006), *available at* http://www.floridabar.org/ (follow "Search" hyperlink; then follow "Ethics Opinions" hyperlink; then search for "06-1").

unnecessarily available confidential information, such as client files stored on a computer that need not be connected to the network for the vendor to perform their duties. Thus, the states in this model partially shift the burden of security from attorneys to the companies with which they contract.

For example, in Maine, non-attorney personnel, such as internet technology professionals, may be employed or contracted to establish and maintain an electronic file storage system without violating client confidentiality.[125] Nevertheless, the attorney remains responsible for the personnel and *their* compliance with the rules of ethics.[126] This regulation imposes no affirmative duty to prevent these vendors from unnecessarily gaining access to confidential electronic data or supervise their conduct.

One of the most permissive models for electronic storage of client files is the Nevada rule. In Nevada, not only may attorneys store client files electronically with few restrictions on his own computer network, but they may also store client records in electronic format *exclusively* on third-party vendor servers across the Internet.[127] This could result in a situation in which a client is located in Los Angeles and his files are electronically stored in New York, potentially creating access and security problems.

A better standard for electronic storage of client documents would render the attorney primarily and proactively responsible for electronic file security. This might require the attorney to isolate certain files or computers on the office network if a third-party vendor requires access to a computer system. By merely stating that an attorney remains responsible for ethical violations but not requiring him or her to take proactive measures to protect client confidentiality from third-party contractors, the weak model states attempt to impose a punitive remedy after the information is disclosed that fails to proactively further the interest of the client.

2. Stronger Model States

The stronger model states are generally more protective of client confidentiality, placing an affirmative, contemporaneous duty of security upon the attorney to preserve confidentiality. Among the leaders in the strong model states, in a 1997 ethics opinion, the Committee on Rules of Professional Conduct of the State Bar of Arizona held that an attorney should exercise care when e-mailing confidential information, and, because of the wide availability

125. Me. Bd. of Overseers of the Bar, Prof'l Ethics Comm'n, Op. 185 (2004), *available at* http://www.mebaroverseers.org/Ethics%20Opinions/Opinion%20185.htm.

126. *Id.*

127. State Bar of Nev., Standing Comm. on Ethics & Prof'l Responsibility, Formal Op. 33 (2006), *available at* http://www.nvbar.org/Ethics/Op%2033%20Electronic%20Data%20storage.pdf.

of encryption programs, the attorney "may want to have the e-mail encrypted" to prevent the "inadvertent disclosure of confidential information."[128] The opinion also noted that e-mail should not be considered to be a "sealed" form of transmission, and should include a disclaimer to that effect.[129] Likewise, Pennsylvania requires an attorney who communicates through e-mail to take reasonable steps to protect client confidentiality,[130] but the Committee on Legal Ethics and Professional Responsibility of the Pennsylvania Bar Association notes that, because of the rapid evolution of technology, the analysis and advice regarding e-mail may change.[131]

Although the stronger model states are in the minority in terms of e-mail restriction and requirements, their policy is more technologically sound. According to a 2006 ABA survey, 48.8% of attorneys use e-mail to send confidential or privileged information to clients at least once per day.[132] Almost 90% of responding attorneys have used e-mail at least twice per year to transmit confidential information.[133] Shockingly, a dismal 16.4% of attorneys used encryption to protect their communication, while 76% relied upon a "confidentiality statement accompanying the transmission" to protect the sensitive data.[134] Only 14.5% of attorneys required their clients to consent to the transmission of their confidential data, and less than 3% required clients to sign a waiver or release.[135] Sixteen percent did not secure the transmission whatsoever.[136] Because of the frequency with which attorneys use e-mail to transmit confidential information and the ease of configuring enhanced security, attorneys should be required to encrypt e-mails that contain confidential information. This additional security protects both the interests of the client and the attorney, and should be considered even by attorneys in states that do not require the additional precautions.

Under the stronger model, the recipients of unintentionally disclosed electronic data may sometimes use it in the course of the case. For example, in three recent ethics opinions, various bar associations in New York analyzed

---

128. State Bar of Ariz., Comm. on the Rules of Prof'l Conduct, Formal Op. 97-04 (1997), *available at* http://www.myazbar.org/Ethics/opinionview.cfm?id=480.

129. *Id.*; *see also* ACLU v. Reno, 929 F. Supp. 824, 834 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997).

130. Pa. Bar Ass'n, Comm. on Legal Ethics and Prof'l Responsibility, Guidance Op. 97-130 (1997), *available at* 1997 WL 816711.

131. Pa. Bar Ass'n, Comm. on Legal Ethics and Prof'l Responsibility, Informal Op. 2005-105 (2005), *available at* 2005 WL 2291093.

132. AM. BAR ASS'N, *supra* note 33, at 51.

133. *Id.*

134. *Id.* at 52.

135. *Id.*

136. *Id.* at 51.

the duties of parties who receive information through e-mail or other electronic means, likely the result of an inadvertent disclosure. In 2002, an ethics opinion issued by the New York County Lawyers' Association stated that an attorney who receives information believing it was not intended for him or her has an affirmative duty to refrain from reviewing the document, to contact the sender, and to comply with the sender's wishes with respect to returning or destroying the document.[137] Nevertheless, this hard line stance softened somewhat in December of 2003, when the Association of the Bar of the City of New York reasoned that, in limited circumstances, an attorney may use information "gleaned before knowing or having reason to know that the communication contain[s] [privileged information]."[138] That stance was reaffirmed and elaborated upon by the New York State Bar Association in 2004.[139]

Washington, D.C., allows good-faith recipients of confidential information to use the data irrespective of the rules of confidentiality. Under this rule, if an attorney is the good-faith recipient of inadvertent information, the attorney need *not* dispose of the document, and "engages in no ethical violation by retaining and using those documents."[140] In other words, an attorney who receives confidential metadata embedded within an otherwise voluntarily transmitted electronic document is prohibited from reviewing the content of the metadata "only where he has actual knowledge that the metadata was inadvertently sent."[141]

Likewise, the State Bar of Arizona considered three alternative approaches for dealing with inadvertent disclosure.[142] It rejected a "lenient" approach, in which inadvertent disclosure is definitively not a waiver of evidentiary privileges, because an affirmative waiver is required.[143] The Bar also rejected

137. N.Y. County Laws. Ass'n, Comm. on Prof'l Ethics, Formal Op. 730 (2002), *available at* http://www.nycla.org/siteFiles/Publications/Publications266_0.pdf.

138. Ass'n of the Bar of the City of N.Y., Comm. of Prof'l & Jud. Ethics, Formal Op. 2003-04 (2003), *available at* http://www.abcny.org/Ethics/eth2003.html.

139. N.Y. State Bar Ass'n, Comm. of Prof'l Ethics, Op. 782 (2004), *available at* http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&TEMPLATE=/CM/ContentDisplay.cfm&CONTENTID=6871.

140. D.C. Bar, Legal Ethics Comm., Op. 256 (1995), *available at* http://www.dcbar.org/for_lawyers/ethics/legal_ethics/opinions/opinion256.cfm.

141. D.C. Bar, Legal Ethics Comm., Op. 341 (2007), *available at* http://www.dcbar.org/for_lawyers/ethics/legal_ethics/opinions/opinion341.cfm.

142. State Bar of Ariz., Comm. on the Rules of Prof'l Conduct, Formal Op. 05-04 (2005), *available at* http://www.myazbar.org/Ethics/pdf/05-04.pdf.

143. Gray v. Bicknell, 86 F.3d 1472, 1483 (8th Cir. 1996) (rejecting the lenient standard, relying upon cases from Florida and Illinois); *see also* State Bar of Ariz., Comm. on the Rules of Prof'l Conduct, Formal Op. 05-04.

a "strict" test, in which waiver is expanded "to all other communications relating to the same subject matter."[144] Instead, the court picked a middle test, in which five factors are considered to determine whether waiver applies.[145] The five factors include the reasonableness of precautions taken, the number of disclosures, the extent to which files were disclosed, the remedial action taken by the attorney, and the interests of justice.[146]

Interestingly, stronger model states allow the receiving party greater latitude regarding the mining and recovery of metadata. For example, in a 2006 ethics opinion, the Ethics Committee of the Maryland State Bar Association unexpectedly rendered a potentially visionary guideline for the use of metadata and inadvertently disclosed information.[147] Under this guideline, Maryland attorneys may use third-party software to scan electronic files that they possess as a result of intentional discovery.[148] This technique could reveal unintended information hidden within the layers of the document.[149] In addition, the recipient of either files containing metadata or files that were otherwise procured as a result of unintentional disclosure need *not* notify the opposing counsel and tell him or her that the information has been discovered.[150]

The stronger model states also require more stringent effort by the attorney to ensure the security of electronically stored documents. In 2005, the Committee on Professional Ethics of the Massachusetts Bar held that, while an attorney could ethically use third-party vendors to "support and maintain a computer software application utilized by the law firm," the attorney must take reasonable steps to ensure that the third parties comply with the rules of confidentiality.[151] Likewise, Pennsylvania allows attorneys to use third-party vendors to service electronic file systems, so long as the attorney takes reasonable steps to ensure that the vendor will protect client confidentiality.[152]

---

144. *Bicknell*, 86 F.3d at 1483 (quoting *In re* Sealed Case, 877 F.2d 976, 981 (D.C. Cir. 1989)).

145. Hydraflow, Inc. v. Enidine Inc., 145 F.R.D. 626 (W.D.N.Y. 1993); State Bar of Ariz., Comm. on the Rules of Prof'l Conduct, Formal Op. 05-04.

146. State Bar of Ariz., Comm. on the Rules of Prof'l Conduct, Formal Op. 05-04.

147. Md. State Bar Ass'n, Comm. on Ethics, Op. 2007-09 (2006), *reprinted in Ethics of Viewing and Using Metadata*, MD. B.J., Mar.-Apr. 2007, at 52.

148. *Id.*

149. *Id.*

150. *See id.* (noting that the new Federal Rules of Civil Procedure may change the way in which this rule is applied).

151. Mass. Bar Ass'n, Comm. on Prof'l Ethics, Op. 05-04 (2005), *available at* http://www.massbar.org/for-attorneys/publications/ethics-opinions/2000-2007/2005/opinion-05-04.

152. Pa. Bar Ass'n, Comm. on Legal Ethics & Prof'l Responsibility, Informal Op. 2005-105 (2005), *available at* 2005 WL 2291093.

New Jersey leads the states in defining the rights and responsibilities attorneys have with respect to electronic storage. A 2006 New Jersey ethics opinion states that electronic storage of client files is not only ethical, but preferable.[153] The Advisory Committee on Professional Ethics reasoned that electronically stored files facilitate more efficient communication with clients because of the enhanced availability, portability, and efficiency of electronic communication.[154] The opinion, however, also discussed the possibility that the information could fall victim to hackers who possess the skills and knowledge necessary to overcome the security protecting the electronic media.[155] Therefore, the opinion holds that an attorney has an *affirmative* duty to take reasonable steps to protect the client's information.[156]

Under the New Jersey rule, just as an attorney must shred files that contain confidential information before they are deposited in the trash, the attorney must ensure that his electronic files are not subject to interception or manipulation.[157] Importantly, the opinion also holds that reasonable care does not require the attorney to absolutely guarantee that the information will not fall prey to hackers, because such a guarantee is impossible even for network professionals.[158] Rather, reasonable care is based upon the technology that is "reasonably available at the time to secure data against unintentional disclosure."[159]

The New Jersey Advisory Committee on Professional Ethics established a two-part test for determining if an attorney has met his or her duty of reasonable care. First, if the attorney has entrusted confidential documents to a third-party vendor, there is "an enforceable obligation to preserve [client] confidentiality and security . . . ."[160] Second, the attorney must use "available technology" to protect client files against "reasonably foreseeable attempts to infiltrate the data."[161] In other words, to satisfy his or her ethical duties under this rule, the attorney must advise any third-party vendors that they must comply with the duty of confidentiality, and the attorney must use technology to avoid "reasonably foreseeable" hacking attempts. Because technology

153. N.J. Advisory Comm. on Prof'l Ethics, Op. 701 (2006), *available at* http://lawlibrary.rutgers.edu/ethics/acpe/acp701_1.html.

154. *Id.*

155. *Id.*

156. *Id.*

157. *See id.*

158. *Id.*

159. *Id.*

160. *Id.*

161. *Id.*

expands and develops so rapidly, an attorney under this model must be agile and adapt to the changes.[162]

Thus, under the stronger model, a state ethics opinion expressly creates an affirmative duty upon the attorney to ensure that electronic files are secure. Likewise, the New Jersey model expressly imposes a duty of network security upon attorneys. Nevertheless, even the New Jersey Advisory Committee on Professional Ethics explicitly declined to define the specific steps that an attorney should take to ethically secure electronic files on a network.[163] Surprisingly, the American Bar Association (ABA) has taken a progressive stance on computer ethics, and the ABA opinions, while not binding, are helpful in determining, from a multistate perspective, the future of the law of computer ethics.

C. The American Bar Association

The American Bar Association has issued some helpful, albeit controversial ethics opinions regarding electronic technology and Model Rule 1.6. In a 1999 ethics opinion, the ABA held that an attorney may typically use unencrypted e-mail to transmit confidential information.[164] The ABA based their determination, in part, upon the reasonable expectation of privacy that attorneys have in their electronic communications.[165] Reasoning that the expectation of privacy in electronic communication is similar to traditional means of message transmission, using e-mail does not run afoul of the Model Rules of Professional Conduct.[166] The ABA's caveat, however, warns that the client should be advised of the dangers of communicating through e-mail, especially when the information transmitted is highly sensitive or prejudicial.[167]

---

162. *See id.* The New Jersey Advisory Committee on Professional Ethics stated:

> In 1983, for instance, when Opinion 515 was published, the personal computer was still somewhat of a novelty, and the individual floppy disk was the prevailing data storage device. The "state of the art" in maintaining electronic security was not very developed, but the ability to prevent unauthorized access by physically securing the floppy disk itself satisfied us that confidentiality could be maintained. By implication, at the time we were less accepting of data stored on a shared hard drive, even one that was partitioned to provide for individual private space for use by different firms, because of the risk of breach of confidentiality under prevailing technology.

Id.

163. *See generally id.*

164. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999).

165. *Id.*

166. *Id.*

167. *See id.*

The dangers of e-mail were highlighted by a speaker in 2005 at the ABA National Conference on Professional Responsibility in Chicago. Arguing that "[t]echnology is a wonderful tool, but like a sharp knife it can be dangerous," speaker David Bloom noted that e-mail is often sent to incorrect recipients despite reasonable effort.[168] Despite the dangers, the ABA and a healthy majority of states take the position that e-mail encryption is not required in most cases. Because of the degree to which the ABA allows attorneys to communicate without encryption, its stance falls under the weaker model of e-mail regulatory schemes.

The ABA's position on metadata differs from that of many states. The ABA surprised many in the legal community in 2006 when the Standing Committee on Ethics and Professional Responsibility issued Formal Ethics Opinion 06-442, holding that attorneys may ethically search for and use metadata hidden within otherwise knowingly disclosed documents.[169] This metadata could lead to the discovery of confidential information.[170] Acknowledging that "lawyers regularly receive e-mail [and other electronic documents] from opposing counsel,"[171] the ABA requires attorneys who inadvertently receive confidential information in the form of metadata to only "promptly notify the sender."[172] In part, the ABA reasoned that attorneys could take reasonable steps to "scrub" the documents of metadata with a simple technological procedure, thereby eliminating the problem.[173] Thus, because a simple, reasonable technical solution exists that should have been employed by the sending attorney, the ABA places the burden upon that attorney to protect the information.[174]

Encouragingly, the opinion offered specific, practical guidance to avoid inadvertently sending documents that contain metadata to opposing parties.[175] To satisfy the ABA's recommendations, first, an attorney should avoid using the "redlining function" of a word processor, which allows the program to track revision changes.[176] Second, an attorney should not "embed" comments within a document, because the comments could later be discovered by the

168. Darshana T. Lele, *Confidentiality: Speakers Reveal Perils and Benefits of Using Technology in Law Practice*, 21 Laws. Man. on Prof. Conduct (ABA/BNA) 310, 310 (2005) (internal quotation marks omitted).

169. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 06-442 (2006).

170. *Id.*

171. *Id.*

172. *Id.* (citing MODEL RULES OF PROF'L CONDUCT R. 4.4(b)) (internal quotation marks omitted).

173. *See id.*

174. *Id.*

175. *Id.*

176. *Id.*

recipient of the document.[177] Third, an attorney should "scrub" the metadata before the document is sent, remaining mindful of any rules that would prohibit altering documents before discovery.[178] Fourth, a confidentiality or protective agreement could be negotiated that would not allow metadata to be used in evidence.[179] Although not listed in the ABA's recommendations, many of the problems associated with metadata in word processing documents can also be avoided by saving the document as an image, which should be done for electronically delivered documents as a best practice, regardless of metadata.[180]

The ABA is fairly permissive in terms of electronic storage of client files. In 1995, the ABA issued an advisory opinion relating to third-party vendors and what access they should have to confidential client information.[181] Holding that the attorney "must make reasonable efforts to ensure that the company has in place, or will establish, reasonable procedures to protect the confidentiality of client information," the ABA states attorneys may employ computer maintenance companies without breaching their duties of confidentiality.[182] Nevertheless, under the rule, the attorney still holds the ultimate responsibility for any breach.[183] No ABA opinions explicitly define the specific steps that an attorney should take to secure electronic client files.

There is no universal bright-line rule that controls the ethics of network security. Nevertheless, based upon the ethics opinions that cover e-mail, inadvertent disclosure, metadata, and electronic storage of documents, a number of conclusions may be distilled. Attorneys owe a duty to their clients to act in conformity with the ethical and professional standards applicable to their respective areas of practice.[184] Failure to conform with these standards can be grounds for malpractice.[185] Computers and technology add an entirely new spectrum to the ethical duties owed to the client. "While computers give tremendous benefits to legal organizations in terms of efficiency, productivity, and delivery of high-quality legal services to clients, they also create

177. *Id.*

178. *Id.*

179. *Id.*

180. If a document is saved as an "image," or picture, there can be no textual revision history contained in the document, since all that is being transmitted is data tantamount to a digital photograph of the document. Image files may include files saved in JPG, PDF, TIFF, and other formats.

181. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 95-398 (1995).

182. *Id.*

183. *Id.*

184. 7 C.J.S. *Attorney & Client* § 47 (2004); *see also* State *ex rel.* Okla. Bar Ass'n v. Champion, 1970 OK 36, 468 P.2d 794.

185. *See Champion*, 1970 OK 36, 468 P.2d 794.

substantial ethical issues."[186] Because there is no universal rule regarding attorney computer security, the ABA has issued some technical recommendations that should at least be considered by attorneys in all states, and should be carefully observed in those states who closely mirror the requirements of the ABA. One state, however, stands above the rest in terms of defining, with a great deal of precision, the explicit steps that an attorney should take to prevent hackers from stealing confidential information. Oklahoma provides the framework by which attorneys can rest assured that their ethical duties are satisfied.

IV. Oklahoma as the Model State

Oklahoma has a strong background in legal technology. It was one of the first states to publish a complete, publicly accessible version of its statutes, ethics opinions, reported cases, and other legal material.[187] Accessible and searchable at no cost, the Oklahoma Supreme Court Network website provides the public with a relatively efficient means of performing state and regional-level legal research.[188] Poised in this progressive stance, Oklahoma allows interested parties to search through ethical codes and opinions online, including materials that help attorneys understand their ethical duties with respect to technology. Further, Oklahoma's embrace of technology in the law is not limited to electronic legal research.

Oklahoma Rule of Professional Conduct 1.1 requires attorneys to "provide competent representation to a client," which includes "the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation."[189] Oklahoma Rule 1.1 is identical to Model Rule 1.1.[190] Several states have interpreted Model Rule 1.1 to impose duties upon attorneys to achieve competency not just with matters of the law, but with the computer hardware and software with which attorneys represent their clients.[191] Thus,

186. ROPER, *supra* note 5, at 43; *see also* MODEL RULES OF PROF'L CONDUCT R. 1.3 (2003) (stating that an attorney has a duty to act with "reasonable diligence and promptness").

187. *See* M.G. Gallagher Law Library, Univ. of Wash., Website of the Week, Feb. 12, 2001, http://lib.law.washington.edu/webweek/2001/Feb122001.html (last visited Jan. 5, 2008).

188. OSCN: The Oklahoma Supreme Court Network, http://www.oscn.net (last visited Jan. 5, 2008).

189. OKLA. RULES OF PROF'L CONDUCT R. 1.1 (2007).

190. *Compare id.*, *with* MODEL RULES OF PROF'L CONDUCT R. 1.1.

191. *See, e.g.*, State Bar of Ariz., Comm. on the Rules of Prof'l Conduct, Formal Op. 05-04 (2005), *available at* http://www.myazbar.org/Ethics/pdf/05-04.pdf ("[A]n attorney or law firm is obligated to take reasonable and competent steps to assure that the client's electronic information is not lost or destroyed. In order to do that, an attorney must be competent to evaluate the nature of the potential threat to client electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end."); Fla. Bar, Prof'l Ethics

although Oklahoma does not explicitly include computer competency in Oklahoma Rule 1.1, the modern trend of Model Rule 1.1 interpretations could require Oklahoma attorneys to achieve competency with the tools used in the law practice. Further, this duty includes "adequate preparation," and can require an attorney to "engage in continuing study and education" to achieve competency.[192] This could require an Oklahoma attorney to participate in continuing education to remain competent in new computer technology.

Addressing computer competency more directly is Rule 1.6 of the Oklahoma Rules of Professional Conduct.[193] The previous version of Oklahoma Rule 1.6(a) provided "[a] lawyer shall not reveal information relating to representation of a client," subject to limited exceptions.[194] For the purposes of computer confidentiality, former Oklahoma Rule 1.6(a) was the same as Model Rule 1.6(a).[195] Former Oklahoma Rule 1.6 imposed an affirmative duty upon the attorney to maintain client confidentiality, stating that "the lawyer must make *every effort practicable* to avoid unnecessary disclosure of information relating to a representation . . . ."[196] Some states have interpreted similar language in the comment section of Model Rule 1.6 as imposing a duty upon the attorney to protect confidential client information stored electronically on computers.[197] As written, former Oklahoma Rule 1.6 did not specifically mention computer technology.

Under recently adopted changes to the Oklahoma Rules of Professional Conduct, however, Oklahoma addresses electronic communication and an attorney's duty to secure electronic client files.[198] Re-adopting Model Rule 1.6(a) with some changes, the recently adopted Oklahoma Rule 1.6(a) reads: "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, [subject to some exceptions] . . . ."[199] Further, two comments to the new Oklahoma Rule 1.6 address the issue of

---

Comm., Op. 06-2 (2006), *available at* http://www.floridabar.org/ (follow "Search" hyperlink; then follow "Ethics Opinions" hyperlink; then search for "06-2"); N.Y. State Bar Ass'n, Comm. on Prof'l Ethics, Op. 782 (2004), *available at* http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&TEMPLATE=/CM/ContentDisplay.cfm&CONTENTID=6871.

192. OKLA. RULES OF PROF'L CONDUCT R. 1.1 cmt. 6 (2007).

193. *Id.* R. 1.6.

194. OKLA. RULES OF PROF'L CONDUCT R. 1.6(a) (2001), *amended by* OKLA. RULES OF PROF'L CONDUCT R. 1.6(a) (2007).

195. *Compare id.*, *with* MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2003).

196. OKLA. RULES OF PROF'L CONDUCT R. 1.6 cmt. (2001) (emphasis added).

197. *See supra* Part III.B.

198. *See* OKLA. RULES OF PROF'L CONDUCT R. 1.6(a) (2007).

199. *Id.*

third parties accessing client information, placing a duty upon the attorney to prevent disclosure.[200]

Comment 16 to the new Oklahoma Rule 1.6 requires a lawyer to "act competently to safeguard [client] information," guarding the data "against inadvertent or *unauthorized* disclosure . . . ."[201] This language of "inadvertent or unauthorized disclosure" is absent from the previous version of Oklahoma Rule 1.6.[202] This additional language may indicate a shift in emphasis by the Oklahoma Bar Association, highlighting the importance of client confidentiality. By holding the attorney responsible for preventing even unauthorized breaches of confidentiality, the proposed rules tacitly require an attorney to secure electronic files from discovery by third parties.

Further, another comment in the new Oklahoma Rule 1.6 places a duty upon the attorney to prevent confidential information from electronically being delivered to unauthorized recipients.[203] Comment 17 states that "[w]hen transmitting a communication that includes [confidential information], the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients."[204] Further, the rule requires the attorney to take "special security measures" if the type of communication does not provide a "reasonable expectation of privacy."[205] To determine if additional security is required, an Oklahoma attorney should consider "the sensitivity of the information and the extent to which privacy of the communication is protected . . . ."[206] Most importantly, under this revision, "the client may require the lawyer to implement special security measures not required by [Oklahoma Rule 1.6]" and may consent to less security than the Oklahoma Rule 1.6 requires.[207]

Although not specifically mentioned, revised Oklahoma Rule 1.6 probably applies to e-mail and Internet-based delivery methods of client documents. Comment 17 discusses "transmitting" a confidential document, departing from language that would indicate mailing or other traditional delivery.[208] Further, the comment places a duty upon the attorney to take "special security measures," which is far more applicable to electronic communications than

200. *Id.* R. 1.6 cmts. 16-17.
201. *Id.* R. 1.6 cmt. 16 (emphasis added).
202. *See* OKLA. RULES OF PROF'L CONDUCT R. 1.6 (2001), *amended by* OKLA. RULES OF PROF'L CONDUCT R. 1.6 (2007).
203. OKLA. RULES OF PROF'L CONDUCT R. 1.6 cmt. 17 (2007).
204. *Id.*
205. *Id.*
206. *Id.*
207. *Id.*
208. *Id.*

traditional methods of confidential delivery.[209] Finally, by requiring the attorney to consider the "sensitivity of the information" and the "extent to which [the communication] is protected," the rule seems to exclude traditionally accepted means of document delivery.[210]

Thus, as the Oklahoma Rules of Professional Conduct have evolved to meet the requirements of modern legal practice, Oklahoma is further poised to lead the states in computer ethics regulation. Nevertheless, Oklahoma's guidance is not limited to formal rules and proposed interpretations. Rather, Jim Calloway of the Oklahoma Bar Association has taken progressive steps to help attorneys merge into a new age of technology. Of particular importance to understanding Oklahoma computer ethics are Calloway's *Oklahoma Bar Journal* articles.

The *Oklahoma Bar Journal* includes practitioner-oriented articles that address the sometimes complex issue of electronic file security. Particularly helpful is an advisory article published in the 1998 *Oklahoma Bar Journal* that discusses the steps prudent attorneys should take to secure the electronic files on their network.[211] In this article, Jim Calloway and Dan Murdock of the Oklahoma Bar Association embrace the advantages of the Internet as a legal tool, noting that "a lawyer who does not have Internet access operates at a substantial disadvantage to his colleagues who do, and, most of the time, does not realize that the disadvantage even exists."[212] Further, Calloway and Murdock outline specific means by which an attorney should protect electronic files from unauthorized discovery.[213] First, a strong password policy is essential.[214] Passwords are sometimes the primary layer of defense between a document and an unauthorized party, and weak passwords can be overcome more easily. Second, backups should be used often and at least one copy should be stored in a location that is geographically separate from the law firm.[215] While many attorneys may understand the importance of backing up electronic files, the technological barriers associated with establishing an automated backup routine prevents some practitioners from adhering to the backup schedule. Thus, an automated backup system is a better means of ensuring the integrity of client files. Third, the attorney should employ a written confidentiality policy that must be signed by all people who have

209. *Id.*
210. *Id.*
211. Jim Calloway & Dan Murdock, *Attorney Advertising in Cyberspace*, 69 OKLA. B.J. 2597 (1998).
212. *Id.* at 2597.
213. *Id.* at 2601-03.
214. *Id.* at 2601.
215. *Id.*

physical access to the files.[216] While this tactic will not affirmatively take information out of the reach of third-party vendors, it at least puts the signatory parties on notice that information discovered therein is confidential and may not be disclosed. Fourth, the attorney should take steps to physically secure the computers that house the electronic documents.[217] Electronic security is of little value if the attorney leaves his notebook computer with confidential information on the courthouse desk, or allows an unscrupulous employee physical access to the physical components of the office computers. Fifth, the attorney should always check references and perform background checks on new or temporary employees.[218] Sixth, policies should be enacted that prevent unauthorized staff from gaining access to unnecessary confidential information.[219] These steps may include, but are not limited to, restricting the rights of the employee user accounts, limiting the hours during which users may connect, and auditing user activities. Each of these six practical recommendations will be discussed and expanded upon in Part V of this comment.[220]

Further, in the November 2006 issue of the *Oklahoma Bar Journal*, Calloway and others explored security tactics that lawyers who use portable computers should employ.[221] Recognizing that personal computers are frequently stolen, the authors argued that attorneys should diligently guard their portable computers to preserve confidential files.[222] In addition, the article suggested that attorneys pay closer attention to USB flash drives and other means of temporary storage that, because of their compact nature, could be easily stolen.[223] These electronic storage devices could later be mined for confidential information. Additionally, this article addressed the issue of metadata indicating that the duty is upon the sending party to ensure client confidentiality.[224] Stating that "[s]ending a document to opposing counsel that potentially exposes the client's comments made while reviewing the document could constitute a major ethical breach," the authors highlight the importance of proactively screening documents for unintended information.[225] This is the

---

216. *Id.* at 2602.

217. *Id.*

218. *Id.*

219. *Id.*

220. *Id.*

221. Ellen Freedman et al., *A Lawyer's Guide to Mobile Computer Security*, 77 OKLA. B.J. 3085 (2006).

222. *Id.*

223. *Id.* at 3088-89.

224. *Id.* at 3086.

225. *Id.* The article makes several suggestions about how sending metadata can be easily avoided, such as creating a clean document, or saving the file in PDF (portable document

better approach, because attorneys who send the information are, or should be, in a better position to protect client files. By placing the burden of maintaining confidentiality on the sending attorney, the authors promote zealous advocacy, client confidentiality, and the adversarial system.

Calloway has addressed numerous other aspects of computer ethics and the practice of law. In 1997, Calloway highlighted the importance of computer disaster recovery and electronic backups of client files.[226] In 2000, he discussed the potential dangers of high speed Internet connections and how the Internet can expose confidential files to hackers.[227] In 2003, he outlined how attorneys can commit "computer malpractice," and some means by which it can be avoided.[228] Finally, in 2005, he explained how any law firm can backup electronic client files, meeting their ethical obligations.[229] Thus, Jim Calloway has helped Oklahoma attorneys better understand the ethical implications of computers in the law office.

Calloway's influence is not limited to *Oklahoma Bar Journal* articles. For the more technologically savvy attorneys, Calloway hosts a blog that contains helpful information about the use of technology in law.[230] These practice tips are invaluable for both technological neophytes and relatively advanced users, and help attorneys bridge the gap between technology and law. Further, Calloway's legal technology practice tips, published on the Oklahoma Bar Association's website, help attorneys understand both the perils and advantages of law office technology.[231]

Although Oklahoma has taken a progressive stance in defining the ethical implications of computer use, potential for improvement still remains. In the future, Oklahoma should publish ethics opinions defining the rights and responsibilities of parties who receive electronic information through misdirected e-mail and metadata. Because the sending attorney has the duty to maintain confidentiality, he or she should bear the burden of ensuring that confidentiality is preserved. This includes, but is not limited to, ensuring that files in e-mails are password-protected, ensuring that the recipients are intended, and ensuring that third parties do not have access to the client's e-

---

format).

226. Jim Calloway, *Are You Prepared for a Real Disaster?*, 68 OKLA. B.J. 3995 (1997).

227. Calloway, *supra* note 24.

228. Jim Calloway, *Malpractice or Ethical Violations with Your Computer*, 74 OKLA. B.J. 3450 (2003).

229. Jim Calloway, *A Backup Proposal for Those Who Know That They Aren't Doing Backup Well*, 76 OKLA. B.J. 2683 (2005).

230. Jim Calloway's Law Practice Tips Blog, http://jimcalloway.typepad.com/lawpracticetips/ (last visited Jan. 5, 2008).

231. Oklahoma Bar Association: Management Assistance Program, http://www.okbar.org/members/map/articles/article_list.htm (last visited Jan. 5, 2008).

mail. If the sending attorney erroneously sends electronic communication to an inappropriate third party, the sending attorney should bear the loss, and the receiving party should zealously represent his or her client and use any information possible from the document. Further, because metadata can be easily eliminated, Oklahoma should allow recipient attorneys to mine electronic documents for hidden information.

In the meantime, absent an all-inclusive, explicit rule, the reasonable practitioner must understand what steps must be taken to secure his or her electronic files. Inherently fuzzy, reasonableness means different things for different attorneys. For example, a large firm should have more resources available to consult third parties regarding network security, while a smaller firm may be required to take preventative measures solitarily. Likewise, whereas an attorney may have a reasonably secure network for dealing with a specific client or set of clients, the security needs may be enhanced if the firm accepts a client with particularly sensitive needs and concerns. Thus, the tools and considerations in Part V should be used to help the attorney both understand his or her duties under the law and take the steps required to secure his or her computer network.

V. Defining Reasonableness—An Attorney's Guide to Understanding the Standards and Recommendations of Computer Ethics and Security

The cornerstone of confidentiality is the idea that an attorney must take *reasonable* steps to ensure that the client's information remains confidential. Thus, the standard can shift depending on the facts and circumstances of each office and each case. The concept of reasonableness is a cornerstone of the legal profession, because it allows for argument on either side of the spectrum. Nevertheless, it is less than satisfying when utilized to help an attorney understand what steps should be taken to shield him- or herself from breaching the rules of ethics. Attempting to draw some practical guidelines, an effective means of measuring reasonableness is weighing the probability and gravity of a hacking attack against the burden which must be undertaken by an attorney to prevent the attack.

Attorneys need not completely withdraw their computers containing client files from the Internet in order to take the requisite "reasonable" steps to protect client confidentiality.[232] While that would certainly satisfy the professional duties of the attorney and minimize the risk of loss, it would

232. State Bar of Ariz., Comm. on the Rules of Prof'l Conduct, Formal Op. 05-04 (2005), *available at* http://www.myazbar.org/Ethics/pdf/05-04.pdf (holding that "[i]t is not unethical to store such electronic information on computer systems *whether or not those same systems are used to connect to the internet*" (emphasis added)).

unreasonably burden business efficiency.[233] Likewise, the solution is not to connect to the Internet without security, despite the ease, because both the gravity and likelihood of attack would increase exponentially.[234] Thus, the solution lies between the two poles.

Just as attorneys cannot ensure that a burglar will not break into their offices and steal information, they cannot absolutely guarantee the safety of electronic files. If the battle between the law firm and the hacker is an intellectual, strategic series of measures and countermeasures akin to a chess match, the end-game for the attorney is to produce a stalemate. Further, "[t]here is no tried-and-true training that can make [an attorney] a security expert, but there are some baseline principles, skills, and tools that must be mastered to become proficient in this field."[235] Too much network security can be expensive, counter-productive, and difficult to implement, while too little security exposes the firm to lost productivity at best, and potential financial liability at worst. By balancing the probability and gravity of attack against the attorney's burden of preventing attack, the attorney can better understand why proactive steps are required, as well as which steps should be taken to secure client files.

A. The Probability of a Hacking Attack and Unintended Disclosure of Confidential Information

Hacking attacks are more prevalent than most attorneys might presume. In a 2006 ABA survey, 14.8% of attorneys indicated that their firm had been attacked by a hacker, up more than 3% since 2005.[236] Shockingly, an overwhelming 39.2% of attorneys did not know if they had been victims of an attack, including 19.8% of solo practitioners.[237] Of the attorneys who reported hacking attacks in 2004 and 2005, 14.3% indicated the attack resulted in the destruction of electronic files.[238] Further, in 2006, 3% of attorneys indicated

233. For example, as long as a secure connection to the Internet can be established, attorneys can remotely access information stored on their office network. This could be invaluable in the event of, for example, forgetting an important document essential for a remote deposition. If secure remote access is properly configured on the network, an attorney can "tunnel" through the Internet, gain access to the office network with proper credentials, copy the file, and use it at a remote location, all within a matter of minutes. This added efficiency also helps eliminate unnecessary billable hours, thereby allowing attorneys to better serve their clients.

234. N.J. Advisory Comm. on Prof'l Ethics, Op. 701 (2006), *available at* http://lawlibrary.rutgers.edu/ethics/acpe/acp701_1.html.

235. KLEVINSKY ET AL., *supra* note 50, at xvi.

236. AM. BAR ASS'N, *supra* note 33, at 35; *see also* AM. BAR ASS'N, *supra* note 8, at 39.

237. AM. BAR ASS'N, *supra* note 33, at 34.

238. *Id.* at 39.

"unauthorized access to sensitive client data," and 4.8% indicated "unauthorized access to other (non-client) sensitive data."[239]

CERT, an organization that tracks and compiles statistical information relating to Internet-based security issues and compromises, lists 38,348 total security vulnerabilities that have been reported from 1995 and the third quarter of 2007, with 5,568 incidents reported in the first three quarters of 2007 alone.[240] More shockingly, the total number of reported incidents of attack against Internet-connected systems was 319,922 from 1988 and 2003.[241] One incident of attack in this report can include from one to thousands of affected computers.[242]

Perhaps because of the aforementioned increasing popularity of wireless networks, even networking professionals can fall victim to expensive hacking attacks.[243] As noted in Part II.B, because of the extraordinary number of wireless network attacks, security is "a practical necessity that has become a reality for today's wireless networks."[244] Determining what the appropriate level of security is for any given wireless network is an essential, practical skill for attorneys who use wireless networks.

Further, while the attacks are becoming more complex, the tools used to facilitate these attacks are becoming easier to use and more readily available. This enhanced availability provides more people that lack specific technical knowledge the ability to perform a malicious attack.[245] Specifically, many effective hacking tools are available for download on the Internet at no cost. For example, *Brutus*, an effective brute-force security cracking program, may be downloaded directly from the developer.[246] *Brutus* may be used to defeat form-based website authentication services. This prevalence of hacking tools increases the probability of attack.

---

239. *Id.* at 35.

240. CERT Statistics: Full Statistics, http://www.cert.org/stats/fullstats.html (last visited Jan. 5, 2008).

241. *Id.* Company websites are one of the most attractive targets for novice hackers; typically the hacker will deface the site in some form, harming the goodwill and professional image (by making customers uncertain of the business's ability to protect confidential information) of the business. Some websites, such as Attrition.org (http://www.attrition.org) track hacked sites and archive images of the defacement; there are thousands of sites in the archive. KLEVINSKY ET AL., *supra* note 50, at 7.

242. CERT Statistics: Full Statistics, *supra* note 240. CERT stopped monitoring these incidents of attack after 2003.

243. VACCA, *supra* note 47, at 164.

244. *Id.*

245. PAQUET & SAXE, *supra* note 51, at 5.

246. *Brutus* is available for download from the developer at http://www.hoobie.net/brutus/.

B. The Severity of Hacking Attacks

Discouragingly, the attacks also seem to be increasing in terms of severity.[247] As just one example, "[i]n the United States alone, $2.6 billion was spent to undo the damage created by the *code red* virus, a malicious worm that exploited a known software vulnerability in certain servers."[248] In addition, "[i]n January 2003, the worm *SQL Slammer* slowed the Internet and infected 75,000 systems in only ten minutes. The net result was damage and cleanup that totaled $1 billion."[249] Further, "[i]n 2004, 74% of all businesses surveyed in the [United Kingdom] reported suffering at least one security incident during the prior year, up from 44% four years earlier," with 68% of these victims claiming that the attacks on their businesses were malicious.[250]

Hacking attacks are especially harmful to law offices, both in terms of actual loss and "collateral damage."[251] While most attorneys might expect losses in the form of destroyed files, the more important losses might include lost client trust.[252] For example, if a client or a potential client notices that an attorney's website has been hacked and defaced, it might make the client less likely to entrust the attorney with highly sensitive confidential information.[253] Because lost revenue and stagnant growth can occur as a collateral loss, the psychological impact on the firm can be more expensive than the lost documents.

Hackers can also allow themselves an opportunity to eavesdrop on what the attorney believes to be private conversations. For example, hackers can install programs and configure options on the computer that allow them to easily regain access to the system. If the computer is equipped with hardware, such as a microphone or a webcam, a moderately skilled hacker can use the attorney's computer like an electronic surveillance device. In the ultimate irony, the attorney seeking to maintain the confidentiality of client information could disclose that information though a hacker's observation of an office meeting over a computer.

C. The Burden of Deploying Network Security

The burden of deploying network security can be great. Like many things in life, there is little to be gained in delusion; constructing and maintaining a secure information technology infrastructure can be costly. The cost required

247. PAQUET & SAXE, *supra* note 51, at 4.
248. *Id.* at 5.
249. *Id.*
250. *Id.*
251. *Id.* at 6.
252. *Id.*
253. *Id.*

to secure a law firm varies wildly, depending upon the degree of security required and the number of computer systems used in the firm. Not surprisingly, only 34.7% of solo practitioners budgeted for technology in 2006, compared to 85.1% in large firms.[254] Of the solo practitioners who did budget for technology, 53.1% allocated less than $2,500.[255] In contrast, at least 6.7% of firms of 100 or more attorneys had a budget in excess of $2 million, with another 11.7% budgeting from $100 thousand to $1.9 million.[256] Consequentially, from 2004 to 2006, approximately 41% of attorneys had no professional technical employees that helped manage the computer systems.[257] 17% employed one person, 8% employed two, 9% employed three to four, and 29% employed "five or more technical support staff."[258]

Because deploying adequate security measures can be expensive, it can be difficult for an attorney, especially a solo practitioner, to justify this cost. This is especially true when a third-party vendor must be employed to ensure an adequate level of security. Particularly unsettling for the frugal attorney is that computer security does not directly produce income or observable results. Unlike purchasing office chairs and stationary, which the attorney may see and touch, the only real measurement of a successful security configuration is the *lack* of a successful hacking attack.[259]

Nevertheless, several facts help constructively reduce the cost of network security deployment. First, while the expenditures can be great at the point of initial deployment, they drop to a near incidental level after this first expense. The primary cost after the initial configuration includes maintaining an adequate level of security.[260] Second, while a law office must deploy a reasonable amount of security, the protection required will not ordinarily be as great as other organizations, such as banks and governmental security departments. Thus, "Fort Knox" security is not necessarily required, and the ordinary firm should be able to deploy an adequate security system for less than $1000.[261] Third, many software tools used to protect and test network security are readily available on the Internet for no cost and others can be

254. AM. BAR ASS'N, *supra* note 33, at 14.

255. *Id.* at 15.

256. *Id.* at 15-18.

257. *Id.* at vii.

258. *Id.*

259. KLEVINSKY ET AL., *supra* note 50, at 1.

260. Some software and hardware vendors, such as Microsoft, offer free updates and patches to correct newly discovered weaknesses or vulnerabilities. Microsoft's updates are available at http://windowsupdate.microsoft.com.

261. If attorneys can take steps to secure their networks unilaterally, the cost of security is dramatically reduced. The $1000 benchmark should cover the cost of an inexpensive hardware firewall, any essential software, and reasonable installation and configuration fees.

licensed for a nominal fee. This ordinarily allows attorneys to shop for the best product and constantly remain vigilant in their network security configuration without consulting a costly third-party vendor. Fourth, the Internet has numerous free resources that can help attorneys understand specific details about network security for law offices, ranging from basic "technology 101" articles to specific, in-depth coverage of specific subject areas. Finally, like other business expenses, the cost of securing a network should be either deducted or capitalized, depending upon the applicable section of the Internal Revenue Code.[262]

Thus, while the gravity and probability of a hacking attack are high, the burden of deploying network security is relatively low. Therefore, deploying network security is a reasonable step that should be taken by an attorney who seeks to preserve his or her clients' confidential information. Nevertheless, while the state ethics opinions are helpful in outlining answers to narrow questions such as whether e-mail encryption is required, or whether files can be stored electronically, few opinions offer direct, practical guidance to law firms who seek to take precise measures to secure their networks. Relying upon the totality of the opinions, Part V.D seeks to define the direct steps that should be taken by an attorney in any state in order to reasonably and ethically secure their networks.

D. Meeting the Burden—Recommended Network and Computer Security

As referenced in Part IV, no states have published an advisory article that fluently and skillfully outlines direct measures attorneys should take to secure their networks other than the *Oklahoma Bar Journal* technology outlines.[263] Because the *Oklahoma Bar Journal* leads the nation in outlining proper, practical security procedures for attorneys, they should be relied upon as a basic framework for network security. Nevertheless, because of the rapid evolution in technology and the importance of client confidentiality, relying upon the articles alone is insufficient to reasonably secure a law office network. To an attorney, it may seem to be a monumental, if not impossible task to manage both the legal and business aspects of a law office, as well as work as a de facto computer professional. However, despite the hype, reasonably securing a computer network does not require a substantial amount of skill or effort. It is "not very hard, or even expensive, [for an attorney] to solve the [security] problem. Usually it's just a silly lapse or laziness that

262. *See, e.g.*, I.R.C. § 162 (2000).

263. *See* Calloway & Murdock, *supra* note 211.

leads to data protection problems."[264] To that end, the following steps should be taken by attorneys who want to protect electronic files.

1. Passwords

One of the most significant vulnerabilities in modern computer systems is weak passwords.[265] Thus, it is essential to implement a strong password policy.[266] Optimally, a user should change his or her password at periodic intervals.[267] Short intervals are better, because "the longer a password is used, the greater the likelihood that it has been compromised.[268] In addition, alphanumeric passwords consisting of eight characters or more should be used whenever possible.[269] Likewise, passwords should absolutely never be a dictionary word, because many hacking programs can, within seconds, crack any password in the dictionary.[270] Obviously, the password should also not be something that may be easily guessed, like a child's name, or that could be easily discovered upon physical examination of the workspace.[271]

The optimal password's characteristics would include an alphanumeric mixture of upper and lower case characters.[272] It should include special characters, preferably toward the middle of the password.[273] A password should not consist of a popular word or phrase, and should exceed eight characters.[274] Password changing policies and schedules can be easily configured in modern Microsoft Windows operating systems. Steps should also be taken to ensure that the system blocks access to the computer for a limited time in the event that a user incorrectly enters a password a suspicious number of times.[275]

---

264. Krause, *supra* note 25, at 25.

265. Weak passwords exhibit some (or all) of the following negative characteristics: (1) short length; (2) all upper or lower-case; (3) all numbers or all letters; (4) non-diverse characters; (5) unexpiring passwords; and (6) comprised of a term that is easily guessed. PAUL REID, BIOMETRICS FOR NETWORK SECURITY 11 (2004).

266. KLEVINSKY ET AL., *supra* note 50, at 41.

267. *See* BILL MCCARTY, LEARNING RED HAT ENTERPRISE LINUX & FEODRA 185 (4th ed. 2004).

268. *Id.*

269. PAQUET & SAXE, *supra* note 51, at 267.

270. KLEVINSKY ET AL., *supra* note 50, at 41.

271. This could include, for example, the practice of writing passwords on post-it notes and storing the notes beneath the keyboard.

272. *See* SUDHANSHU KAIRAB, A PRACTICAL GUIDE TO SECURITY ASSESSMENTS 396 (2005).

273. *Id.*

274. JACK J. CHAMPLAIN, AUDITING INFORMATION SYSTEMS 145 (2d ed. 2003).

275. Multiple incorrect guesses can indicate a potential hacking attempt. A "group policy" can be set to lock an account should this occur. To configure group policy in Windows XP, open the Group Policy Editor and navigate to Computer Configuration/Windows

An attorney who fails to configure a strong password system can allow a hacker to gain access to confidential client information. Because even an unauthorized user can gain access to confidential files with the correct password, ensuring compliance with these password recommendations is vital. By enforcing a strong password policy, an attorney will have taken the first step to reasonably secure electronic files. Nevertheless, additional security must also be configured.

2. Backups, Disaster Recovery, and Data Redundancy

One of the most important things that an attorney can do is develop a data redundancy plan.[276] Nevertheless, few attorneys follow backup plans.[277] In a 2006 ABA study, only 25.8% of responding attorneys indicated that backups were performed daily.[278] Over sixty percent of the responding attorneys reported their firm backed up data in intervals of one week or greater.[279] Larger firms backup data more frequently than smaller firms. While 4.5% of firms with over 100 attorneys backup their information more than twice daily, only 1.9% of solo practitioners are this cautious.[280] This disparity could be due to additional technological resources or enhanced need.

Not surprisingly, larger firms also use more robust backup practices. Fifty-five percent of solo practitioners use optical drives, such as writable CDs and DVDs, to backup information.[281] The danger with this method is that the media is fragile, and anything from an office fire to a scratch could eviscerate the backups. Only 12.2% of firms with fifty to ninety-nine attorneys, and 3% of firms with 100 or more attorneys prefer this method.[282] However, attorneys in small firms are more aware of the data backup policies than attorneys in larger firms.[283] While only 5% of the solo practitioners were unaware of what type of media was used for backups, a whopping 73.7% of the large firm attorneys remained ignorant.[284] This difference is probably the result of the

---

Settings/Security Settings/Account Policies/Account Lockout Policy and define the account lockout duration to be at least a few minutes, and the threshold to be less than five invalid logon attempts. *See* Implementing and Troubleshooting Account Lockout, http://www.windowsecurity.com/articles/Implementing-Troubleshooting-Account-Lockout.html (last visited Jan. 5, 2008).

276. Krause, *supra* note 25, at 31.
277. *Id.*
278. AM. BAR ASS'N, *supra* note 33, at 38.
279. *Id.*
280. *Id.*
281. *Id.*
282. *Id.*
283. *See id.*
284. *Id.*

ability of large firms to hire networking and data professionals to configure and complete a data backup system.

Shockingly, 46.2% of attorneys in law firms either do not have or do not know if they have a disaster recovery plan.[285] Cost seems to influence these figures. While 57.4% of solo practitioners, nearly as high a percentage as the largest firms, have disaster recovery plans, there may be weaknesses in how the plans are formed.[286] For example, while no firms of ten or more attorneys report placing an associate attorney in charge of protecting the information, over 90% of solo practitioners are responsible for performing their own backups.[287] This could be expensive in terms of time if not managed properly.

Because cost is a factor, an attorney's backup schedule will depend heavily upon the type of firm in which he or she practices. When determining the frequency by which backups should be performed, the attorney should consider how much work he or she is willing to lose.[288] An inappropriate backup schedule can expose an attorney to disaster in the event of a hacking attack, viral infection, or environmental disaster.[289] "Large law firms [should ensure] that information is saved on file servers, backed up daily and stored off-site at a secure location."[290] For other firms, if off-site backups are not an option, the attorney should consider storing data on rotating tape backup drives that can be stored in a fireproof safe. At a minimum, copies of files should be transmitted to temporary media, such as USB or CD-RW discs, or to a portable hard drive. Backing up files does not have to be expensive, or even especially difficult. Microsoft has published a tutorial on Windows XP's integrated backup utility, and other backup scheduling software is available.[291] With a properly configured backup system, the data should be protected with virtually no additional effort.[292]

At least one court was unwilling to forgive an attorney whose computer negligence resulted in the destruction of client files. In the case of *In re Ward*, a North Dakota attorney accepted $6000.00 as a retainer for a case.[293] In 2003, when the representation was complete, the attorney claimed the fee, but could

285. *Id.* at 37.
286. *Id.*
287. *Id.*
288. Krause, *supra* note 25, at 31.
289. *Id.*
290. *Id.*
291. For Microsoft's recommendations on using the Windows XP backup tools, see Windows XP: Back Up Your Files, http://www.microsoft.com/windowsxp/using/setup/maintain/backupfiles.mspx (last visited Jan. 5, 2008).
292. *See generally id.*
293. *In re* Ward, 701 N.W.2d 873 (N.D. 2005).

not produce his record of time on an invoice.[294] The physical files documenting the time spent were taken by a person with a power of attorney for the client, the attorney claimed.[295] The electronic documents were destroyed by a computer virus.[296] Finding that the destruction of his records by a virus did not relieve the attorney of his ethical obligations, the court issued him a reprimand and a fine.[297]

Thus, in order to protect client files, an attorney must establish a means by which electronic files may be recovered in the event of a loss.[298] Any backup policy is better than none, thus, an attorney should at least back up files on removable media, such as CD-RW, DVD-RW, or USB storage devices.[299] Ideally, firms should enact robust backup procedures that protect client information from the dangers of hackers, viruses, and environmental disasters.[300] Nevertheless, an attorney must also ensure that his or her computers that contain electronic client files are secure.

3. Physical Security

Despite the complex network security measures that are enabled to prevent an unauthorized user from remotely accessing resources, if an unscrupulous person is able to gain physical access to an improperly secured machine, the person can perform a tremendous amount of harm in a small amount of time. For example, a Linux LiveCD[301] may be used to mount the file system that was previously secured by a password because the CD loads a small Linux operating system in memory. This can result in a catastrophe, because the attackers have access to all of the information that was previously shielded by a user password.[302] The attacker also has the opportunity to either clear the administrator password or steal the Windows "hash" files, which can be later

294. *Id.* at 874-75.
295. *Id.* at 877.
296. *Id.*
297. *Id.*
298. *See* Calloway, *supra* note 226.
299. *Id.*
300. *See generally* Krause, *supra* note 25, at 31.
301. A LiveCD is a bootable version of Linux designed to operate in temporary memory space. One consequence of using a LiveCD is that a user need not have privileges to install software in order to use the LiveCD. In fact, anyone with physical access to the machine and the ability to boot the computer from the CD-ROM drive can become an administrator by using a LiveCD. Many types of LiveCDs exist, including the popular Ubuntu operating system series. Ubuntu can be downloaded from http://www.ubuntu.com.
302. *See* G4, Dark Deal: Windows Password Hacking, http://www.g4tv.com/screensavers/features/664/Dark_Deal_Windows_Password_Hacking.html (last visited Jan. 5, 2008).

decrypted to reveal the administrator's passwords.[303] After an administrator's password has been compromised, the potential for lost data is almost limitless. A skilled hacker can use the credentials to remotely access client files, delete information, send e-mails and other information on behalf of the attorney, and execute an array of other frightening and malicious attacks.[304]

For all of these reasons, physical security is imperative. First, the system BIOS[305] should be configured so that a user may not boot from an external device.[306] In addition, a BIOS password should be enabled so that users cannot make changes to this configuration.[307] Next, the attorney should consider implementing a hard drive password system, which can prevent data from being compromised if the drive is stolen.[308] Finally, the attorney should ensure that tamper-resistant screws are installed in your computers to prevent theft of components that might hold confidential information.

4. Hardware & Security

Firewalls are important components of any computer security system, because they restrict the type of network traffic that can come in and out of the network.[309] Firewalls are discussed in detail in Part II.A, and vary widely in configuration and functionality. Hardware firewalls typically offer the best protection, but a number of software firewalls have been developed for use by the average consumer.[310]

Large firms may need to hire a network professional to configure firewalls for advanced operation. In addition, large firms can use proxy servers to prevent employees from reaching certain websites and from conducting certain activities on the Internet.[311] Smaller firms, however, should be adequately

303. *See id.*

304. To make things more complicated, a hacker with such credentials can make it very difficult to discover the origins of his attack; he can clear the server logs each time he accesses the computer remotely.

305. The BIOS of a computer controls the computer's hardware at a lower level than the operating system. This means that, despite any access restrictions in the operating system, a person with access to an unsecured BIOS can configure the computer to access external devices before attempting to access the operating system. This can result in a breach of security, since any security configured within the operating system will never have the opportunity to be initialized.

306. BIOS configuration is slightly different for each model of computer; consult your motherboard or computer manufacturer's documentation for specific details.

307. *See generally* Calloway, *supra* note 24.

308. One vendor of a hard drive password solution is Magiclab. *See* StorageCrypt, http://www.magic2003.net/ (last visited Jan. 5, 2008).

309. *See* Calloway, *supra* note 24, at 1713-14.

310. *See generally id.*

311. For a detailed description of proxy servers, see Microsoft ISA Server: Previous

protected with software firewalls,[312] or inexpensive routers with integrated firewalls.[313] These products are generally available for less than fifty dollars.[314]

When traditional security is not enough, an attorney should consider employing biometric authentication. The three main methods by which identity can be established are examining something you know, such as a password, something that you possess, such as a magnetic slide card or access token, and something you are, such as a biological trait.[315] "Digital certificates, public [keys], biometrics, and smart cards are all examples of authentication methods that are generally considered very secure."[316] Biometrics offer an expensive, but considerable, security advantage.[317] In a system that uses biometrics,[318] after information is collected from the user in a recording process, the physiological trait will be used to authenticate the user on the computer or network.[319] Examples of biometrics include "passive" measures, like the user's "face, voice, gait, and . . . eye [measurements]," and "active" biometrics such as "finger, hand, and vein biometrics . . . ."[320] Biometrics are inherently more secure than password-based security structures because passwords always have the potential to be guessed, and biometrics are very difficult to falsify.

Biometric security can also be justified in terms of return on investment (ROI). In *Biometrics for Network Security*, Paul Reid examines the ROI that can be expected from various means of biometric security implementation. Finger biometrics earn an ROI rating of 7 out of 10 because of the minimal cost of the finger reading hardware and "the ease of deployment and training . . . ."[321] Face recognition earns a much lower 5.5 ROI rating, because it requires high-definition cameras and presents significant deployment costs.[322] Voice biometrics also earn a ROI rating of 5.5 because the microphone equipment is susceptible to interference that reduces its practical

---

Versions, http://www.microsoft.com/isaserver/prodinfo/previousversions/default.mspx (last visited Jan. 5, 2008).

312. *See* Calloway, *supra* note 24, at 1713-14.

313. *Id.*

314. *Id.*

315. REID, *supra* note 265, at 10-14.

316. KLEVINSKY ET AL., *supra* note 50, at 42.

317. *See id.* at 42-43, 435.

318. Biometrics are "physical or psychological trait[s] that can be measured, recorded, and quantified." REID, *supra* note 265, at 5.

319. *Id.* at 6.

320. *Id.* at 36.

321. *Id.* at 127.

322. *Id.* at 130.

reliability.[323] Iris biometrics, or, "scanning" the eye, scored a lower ROI rating of 4.5, because the cost of implementing eye-scanning hardware is relatively high, and special lights are required for proper ocular illumination.[324] Thus, the fingerprint biometric option is the "closest overall to being ideal . . . ."[325] A USB Microsoft fingerprint reader is available for around forty dollars.[326]

5. Software Security

a) Employees & Group Policy

While a hacker can attempt to gain access to confidential information through specific network vulnerabilities, the greater danger may be from within the firm's own walls. "[S]imply having a security system isn't enough . . . ." to protect an attorney from liability.[327] Rather, an employee security policy must be enforced.[328]

Employers in other industries have expressed concern of attacks by their employees. For example, one-third of respondents to a study by *Disciplined Security* were concerned about attacks from their own employees.[329] This falls just below the number of employers who feared attack by outsiders.[330] In addition, employee good faith was not necessarily the determining factor. It was not that employers mistrusted their employees as much as they were concerned that the employees "might import infected codes . . . and introduce them to the company network."[331] As further evidence of this fact, a report published in 2004 found that small businesses (from one to forty-nine employees) experienced 53% of their network threats from internal sources.[332]

Thus, dangerous employees need not act maliciously. Instead, they can be dangerous if disgruntled, careless, or angry.[333] Because employees can become an ethical hazard, employee password and resource access should be allocated sparingly.[334] Specific security permissions should be the exception,

323. *Id.* at 133.
324. *Id.* at 136.
325. *Id.* at 138.
326. For inexpensive fingerprint readers, see PriceScan.com, Microsoft Fingerprint Reader USB, http://www.pricescan.com/items/item161599.asp (last visited Jan. 5, 2008).
327. *See* Krause, *supra* note 25, at 31.
328. *Id.*
329. PAQUET & SAXE, *supra* note 51, at 6.
330. *Id.*
331. *Id.*
332. *Id.* at 12.
333. *Id.* at 11.
334. *See id.*

not the rule.[335] An attorney should at least ensure though Windows group policies and NTFS[336] file security that any employee accounts are limited in scope, and cannot modify, install, or remove files that are not in accordance with the employee's job duties.[337] Employee accounts should require strong passwords, and the employee should be required to change his or her password at specific intervals.[338] Employee accounts should not have sufficient permissions to install software, and the attorney should remain vigilant to the presence of any third-party file sharing software, which could automatically index and share the law firm's files with millions of clients on the Internet.[339]

Because employees already have a computer that is considered internal to the network, it is easier for the user to exploit his or her limited network access and acquire access to protected information.[340] Likewise, users may establish other connections to the Internet, such as installing a modem or remote connection software, that will render the network much less secure.[341]

An employer can also remotely observe an employee's session, if such practice is allowed by local law. Remotely observing a user's session allows the employer to eavesdrop on the user's activities without the user's knowledge. For example, the employer could stealthily watch as a user sends an e-mail, browses the Internet, or plays games. Not only could the information itself prevent a catastrophic situation, but the deterrent effect is substantial. An employee who knows his activities may be watched and recorded will probably be less likely to engage in unethical or otherwise undesirable behavior.

b) Microsoft Windows Updates

The vast majority of law firms use Microsoft operating systems on their office computers.[342] At 75.2% of the install base, Windows XP is the most commonly used operating system, followed by Windows 2000 at 12.2%.[343] Less than 3% of attorneys use alternative operating systems, such as Mac OS

335. *See id.*

336. NTFS is an acronym for the Windows NT File System, under which attorneys can define which users have the right to edit, delete, or read files.

337. *See id.*; *see also* Calloway, *supra* note 24.

338. *See supra* Part V.D.1.

339. Krause, *supra* note 25, at 31; *see also* Calloway, *supra* note 24.

340. *See generally* KLEVINSKY ET AL., *supra* note 50, at 5-50.

341. This is intuitive; if a firewall is installed at the "door" to the Internet, by installing a modem or remote connection software on an individual machine in the network, an alternate entrance to the network is available, essentially leaving a back door into the network which may be exploited. *Id.* at 72.

342. *See* AM. BAR ASS'N, *supra* note 26, at 39.

343. *Id.*

or Linux.[344] Thus, it is vital for an attorney to download and install the security patches that Microsoft releases to correct problems detected in their software.

Microsoft updates are available at no charge through Microsoft's updating service on their website.[345] Updates require little effort to install and configure, and most of them configure themselves.[346] Further, after automatic updates have been configured, the computer will retrieve and install the updates automatically, which saves the firm time and money.[347] Thus, Microsoft updates are perhaps the least burdensome and the most helpful tool to prevent hackers from gaining access to confidential files, and failure to install the updates is inexcusable.

c) Antivirus and Anti-Spyware Software

Although many people may understand that viruses can infect computers, attorneys might be surprised at the degree in which law offices fall victim to viral attacks. In a 2005 report, the ABA revealed that 70.9% of attorneys reported their firms were the victims of a viral attack.[348] The rates of infection were relatively proportional to firm size, with solo practitioners reporting an infection rate of 50%, and firms of 100 or more attorneys reporting infections at 81.6%.[349] And all sixteen responding attorneys from firms between fifty and ninety-nine attorneys reported a viral attack at their firms.[350]

The rates of damage reflected in the survey were also substantial. Over 35% of attorneys reported some significant damage or business loss.[351] While 8.8% of the attorneys reported destroyed or lost files, more substantial damages occurred in a small minority of attorneys.[352] Specifically, 0.5% of responding attorneys reported "[u]nauthorized access to sensitive client data."[353] Thus, to protect client files and client confidentiality, an attorney must attempt to prevent viral infection. A number of companies market inexpensive antivirus software, and some programs, such as AVG Antivirus, offer consumer licenses at no cost.[354]

---

344. *Id.*

345. For a detailed discussion of Microsoft Windows Updates, see Microsoft Windows Update, http://windowsupdate.microsoft.com (last visited Jan. 5, 2008).

346. *Id.*

347. *Id.*

348. AM. BAR ASS'N, *supra* note 30, at 40.

349. *Id.*

350. *Id.*

351. *See id.*

352. *Id.*

353. *Id.*

354. For AVG licensing requirements and terms of use, see AVG Anti-Virus and Internet

6. Wireless Networking

George Riemer, General Counsel and Deputy Director of the Oregon State Bar, defined a series of steps that should be performed to increase expectation of privacy in an attorney's wireless network.[355] Riemer suggests that attorneys begin by asking themselves if they actually need a wireless network, especially if a wired network is already in place.[356] Quite possibly, the small amount of utility offered by a wireless access point pales in comparison to the substantial increase in risk inherent in wireless networks. Further, Riemer states that attorneys should modify the default factory settings on their wireless access point, which prevents unauthorized persons from changing settings in the router using the default credentials.[357] This is absolutely fundamental and should be performed in any wireless network installation and configuration. By failing to change the default information, not only can attorneys allow a third party to remotely connect to and administer the wireless access point, but the third party can actually *exclude* the valid users. Third, Riemer advises that wireless encryption security should be enabled; he suggests enabling 128-bit WEP[358] encryption, which seemed to be a valid choice in 2004 when the article was written. Now, however, a far more secure method of encryption, such as WPA, should be used.[359] Finally, Riemer suggests MAC address filtering, which, in theory, will prevent unauthorized wireless adapters from associating with your wireless access point, thereby rendering them unable to communicate with your network.[360]

Security, http://www.grisoft.com (last visited Jan. 5, 2008).

355. George A. Riemer, *The Invisible Door: Confidentiality Meets Wireless Technology*, OR. ST. B. BULL., July 2004, at 23, 24.

356. *Id.*

357. *Id.*

358. WEP is an acronym for "Wired Equivalent Privacy." It is a feature that can be used to encrypt information on a wireless network. *See* Jeffrey Dingle, *How Secure Is Your Wireless Security?*, SECURITY, Jan. 2007, at 34, 35.

359. *See* Sylvia Walsh-Flaherty, *Wireless Networking Making a Big Impact*, ELECS. WKLY., June 13, 2007, at 26, 27. WPA is an acronym for "Wi-fi Protected Access." *Id.* WPA is still vulnerable to hacking attempts if a weak password is used. In order to facilitate more robust security, a long password with letters, numbers, and special characters should be used. *See supra* notes 272-74 and accompanying text.

360. MAC filters are a great level of initial defense. However, hackers can use a simple tool to scan the wireless traffic and determine which valid clients are communicating with an access point. After a valid client is discovered, the hacker can clone the MAC address of the client, thereby gaining access to the network. For this reason, MAC filtering in and of itself is an insufficient form of network security. *See supra* note 41 and accompanying text.

Further, at least one state has proposed a regulatory solution for wireless security problems. In a surprising development, California "has become the first legislative body in the world to pass legislation requiring wireless equipment manufacturers to warn consumers about the dangers of using unsecured wireless connections."[361] Finding that as many as two-thirds of wireless networks in the City of Los Angeles are not secure, the law will require manufacturers of wireless devices to include, potentially with stickers on the product boxes or setup software, warnings of the risks associated with an unsecured wireless network.[362]

As a best practice, wireless internet security will include some form of HTTP[363] authentication that requires a user already associated with the access point to enter a username and password to browse the Internet. Nevertheless, the wireless network may still be vulnerable to attack.[364] HTTP is relatively effective at validating usernames and passwords, but the information is sent in relatively easily decodable format.[365] For example, a hacker may use software to conduct an HTTP authentication attack that attempts to guess the password through a list of probable matches or through brute force.[366] Because password guessing is somewhat inefficient, the most appropriate countermeasure for bypassing HTTP authentication is a strong password policy.[367]

In any scenario, a strong wireless password should be used with a variant of WPA security, because WEP security is easily defeated.[368] In addition, MAC address filtering should be enabled, which limits the computers that are authorized to associate with the access point.[369] Access restriction can be further reduced in the access point firmware, such as limiting the hours in which clients may associate wirelessly with the network, and wireless networks can be rendered relatively secure.[370] Nevertheless, attorneys should

361. *Wifi Security to Become Law in California*, WIRELESS AM. DAILY BULL., Sept. 4, 2006, *available at* Westlaw, 2006 WLNR 15316395.

362. *Id.*

363. HTTP is an acronym for HyperText Transfer Protocol, and is used in web-based authentication forms. *See* YOUNG & AITEL, *supra* note 10, at 463.

364. *See generally* Riemer, *supra* note 355.

365. YOUNG & AITEL, *supra* note 10, at 463-502.

366. Common programs used to bypass HTTP-based authentication include *Hydra*, *TeeNet*, and *Brutus*. Each of these programs use either brute force, dictionary attacks, or a combination thereof to attempt to guess an Internet-based method of authentication. They are also free and readily available on the Internet. *See* STUART MCCLURE ET AL., HACKING EXPOSED 216-17 (5th ed. 2005).

367. JOEL SCAMBRAY ET AL., HACKING EXPOSED WEB APPLICATIONS 129 (2d ed. 2006).

368. *See supra* Part II for a discussion of wireless networks.

369. SCAMBRAY ET AL., *supra* note 367.

370. *Id.*; Riemer, *supra* note 355, at 24; *see also supra* Part II.

ensure that they truly need a wireless network before configuring a wireless access point and weakening network security.[371]

7. Metadata & File Deletion

Sometimes an attorney may need to permanently delete confidential data. Nevertheless, permanently deleting information is not easy. If an attorney desires to delete a file permanently, merely pressing the delete key will not perform the task.[372] The problem lies with the way in which files are stored on a hard drive.[373] Because the drive uses magnetic storage, information is contained on metal platters much like the way data is stored on the ribbon on a cassette tape.[374] The computer tracks where the files are stored on the hard drive, much like an index.[375] When the user orders the operating system to "delete" the file, a command is executed that removes the address of the file in this index.[376] Although the computer "forgets" where the file is stored on the drive, the file itself is still magnetically present.[377] Until additional data is written over the old data, the old data may still be recovered by using widely available and relatively inexpensive software.[378]

Clearly, this could pose substantial problems to client confidentiality in the event of the theft, sale, or other disposition of older computer hardware. If the attorney has failed to take the appropriate steps to remove the data magnetically stored on the drive, it could be recovered and disclosed to third parties. This could result in identity theft and a breach of confidentiality.

In order to permanently delete information from a drive, several applications are available. Utilities are sometimes provided by the hard drive manufacturer that can perform an unconditional format of the drive.[379] Further, "[d]ata erasing programs can be bought for $50 . . . ."[380] Some analysts have taken a harder line to data stored on hard drives, claiming, "The only way to completely erase a hard drive is to take it out of the computer and

371. Riemer, *supra* note 355, at 24.

372. Krause, *supra* note 25, at 31-35.

373. *Id.*

374. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 539 (2005).

375. The old method of tracking files is by the File Allocation Table (FAT). Modern techniques have evolved, but these techniques still track file location and other data. David F. Rxelrod et al., *Hard Times with Hard Drives: Paperless Evidence Issues That Can't Be Papered Over*, CHAMPION, Aug. 2001, at 18, 20.

376. *Id.*

377. *Id.*

378. *Id.*

379. *See* Krause, *supra* note 25, at 31.

380. *Id.*

smash it with a hammer . . . ."[381] While this dramatic step is overkill, it punctuates the importance of correctly destroying electronic files.

An attorney who sends an electronic word processing file may also be in danger of inadvertently relaying confidential information to the receiving party through metadata. "The risk of inadvertently transmitting what a lawyer knows is confidential information to an opposing or third party has always existed. Not too long ago, the primary risk was that a letter intended for a client would instead be mailed or faxed to opposing counsel."[382] The danger now is data that is hidden within electronic copies of documents that can be "mined," potentially exposing confidential client information.[383]

Metadata can yield relatively little or extraordinarily harmful information.[384] For example, a file may contain only the date of creation and the name of the author.[385] Likewise, the file may contain such vital and damaging information as "the names of everyone who has worked on or seen a specific document, text and comments that have been deleted and different drafts of the document."[386] However, metadata can be minimized or eliminated. Microsoft has released a tool that is designed to remove metadata from Microsoft Word documents.[387] In addition, metadata can be minimized by saving the file in RTF, PDF, JPG, or similar format.[388]

---

381. *Id.* (internal quotation marks omitted). This author does not recommend the hammer-smash method; the physical structure of the drive could be destroyed, only to have the internal platters re-mounted in a different drive frame. This would allow a third party to read the data on the drive. As an extreme example of the abuses a hard drive can withstand, *PCPro*, a British online news magazine, recently conducted an experiment where a hard drive was thrown across an office several times, slammed onto a desk, and submerged in a pot of sugary, boiling hot tea for five minutes. By transferring the platters from this hard drive into another hard drive frame, OnTrack, a commercial data recovery company, was able to recover all of the files from the damaged hard drive. *See What Does It Take To Destroy a Hard Disk?*, PCPRO, May 16, 2007, http://www. pcpro.co.uk/features/113080/what-does-it-take-to-destroy-a-hard-disk.html.

382. David Hricik, *I Can Tell When You're Telling Lies: Ethics and Imbedded Confidential Information*, 30 J. LEGAL PROF. 79, 79 (2006).

383. *See supra* Part II.A.

384. *See supra* Part II.A.

385. *See supra* Part II.A.

386. Jason Krause, *Hidden Agendas: Unlocking Invisible Electronic Codes Can Reveal Deleted Text, Revisions*, A.B.A. J., July 2004, at 26, 26; *see also supra* Part II.A.

387. The metadata removal tool can be found by searching Microsoft's website. *See* Microsoft Corporation, http://www.microsoft.com (search for "rhdtool.exe") (last visited Jan. 5, 2008).

388. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 442 (2006).

8. E-mail

States differ widely as to which standard should be applied to e-mail. Most states allow attorneys to transmit confidential data in unencrypted e-mail absent special circumstances. Some require written consent of the client before the client's information is electronically transferred, while others mandate prudence and caution.[389] The various interpretations of what security measures are required in terms of e-mail are helpful in determining what steps should be taken to reasonably secure one's network, but not determinative.

As a general rule, the attorney should take care that the recipient of a confidential e-mail has a secure receiving location.[390] Other parties should not have ready access to the recipient's e-mail. In addition, it may be worth the slight configuration burden to enable some light form of encryption.[391] Even light encryption would make intercepting and reading e-mail more difficult.[392] Finally, if an attorney sends a document through e-mail, he or she should take the extra time required to password-protect attached files, which is a service available in all modern word processing systems.[393]

Thus, while the attorney must take what seem to be many steps to ensure network security, the steps are small and the road is relatively smooth. By following the guidelines in Part IV, attorneys can be relatively confident that their electronic files are secure. Likewise, attorneys will have taken reasonable steps to secure the confidentiality of client files, and will have satisfied their rules of ethics.

VI. Conclusion

Attorneys' fundamental duties to clients have not been altered by the advent of computer technology. Nevertheless, the rules of ethics must adapt to the

389. *See* State Bar of Ariz., Comm. on the Rules of Prof'l Conduct, Formal Op. 97-04 (1997), *available at* http://www.myazbar.org/Ethics/opinionview.cfm?id=480 (noting lawyers should use e-mail cautiously, consider encryption, and include a cautionary statement that information is confidential); S.C. Bar Ass'n, Ethics Advisory Comm., Op. 97-08 (1997), *available at* http://scbar.org/member/opinion.asp?opinionID=469 (holding lawyers may communicate with clients via e-mail but should discuss encryption options). *But see* Iowa Sup. Ct. Bd. of Prof'l Ethics and Conduct, Op. 97-01 (1997), *available at* http://www.iowabar.org/ethics.nsf/ (follow "Iowa Board of Professional Ethics Opinions" hyperlink; then follow "09/18/1997 97-01" hyperlink) (stating client must give written consent to transmission of information by e-mail or Internet, and only after disclosure of potential for loss of confidentiality).

390. *See supra* Part III.C.

391. *See* State Bar of Ariz., Comm. on the Rules of Prof'l Conduct, Formal Op. 97-04.

392. *Id.*

393. *See* Calloway & Murdock, *supra* note 211, at 2601.

new realities of the law office. Because the standard of maintaining client confidentiality is based upon reasonableness, an attorney has a duty that has expanded to envelop a wide range of technology that, perhaps a decade ago, would have never been contemplated. The duties owed by attorneys to clients are substantial, and the risks of breaching these duties are real. To take no action to prevent hacking and protect electronic files is to virtually ensure ethical responsibility. Thus, a reasonable amount of security must be configured on each computer network that contains confidential information and is exposed to the public through either an Internet connection or a wireless network configuration. By taking these steps, attorneys can evade liability for the disclosure of client information that has been electronically stolen. As more attorneys begin to use networking equipment, more firms and clients will be exposed to attack. It is expected that, as case law develops, courts will hold that attorneys who follow the recommendations, strategies, and reasonableness analysis in this comment will have satisfied their ethical standards.

Nevertheless, until more cases are heard, attorneys must continue to speculate on precisely which conduct is acceptable, and which is not. As is often the case in life, with respect to the question of computer ethics, perhaps practical wisdom is best:

> Technology malpractice suits are rare, and they can be kept that way if lawyers don't make dumb mistakes that, offend or upset their clients. Keep the clients happy and always let them make decisions about how you'll use technology to represent them . . . . Happy, informed clients don't sue their attorneys.[394]

Ash Mayfield

394. Krause, *supra* note 25, at 46 (internal quotation marks omitted).